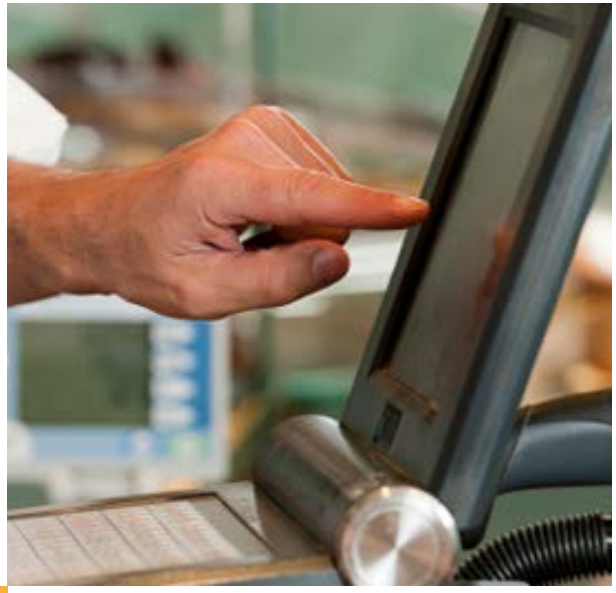
securityMETRICS®

Ebook

HOW TO PREPARE FOR A PCI DSS AUDIT

8 TOP COMPLIANCE TIPS FROM QSAS



HOW TO PREPARE FOR A PCI DSS AUDIT

8 TOP COMPLIANCE TIPS FROM QSAS

INTRODUCTION

Payment Card Industry Data Security Standard (PCI DSS) audits are often seen as a necessary evil. But PCI DSS auditors want you to succeed in compliance and data security.

In this ebook, 8 Qualified Security Assessors (QSAs) from SecurityMetrics offer their best recommendations on how to save time on your next PCI DSS audit and maintain PCI compliance.

"Maintain an accurate network diagram. I often see diagrams that represent a PCI compliant network, but actual network configurations usually reflect otherwise."

-Thomas McCrory, QSA, CISSP

1 MAINTAIN AN ACCURATE NETWORK DIAGRAM

Accurate network diagrams are vital because they show how your systems interact with card data. Systems in your network that store, process, or transmit card data need to be properly secured and separated from other systems on your network.

Many merchants have big flat networks with a firewall at the edge, but that's it. Everything inside the network is connected with each other. Flat networks make securing card data extremely difficult because your entire network is in scope for PCI.

To avoid network problems, you should create a diagram that shows how cardholder data enters your network, the systems it touches as it flows through your network, and any point it may leave your network (e.g., sent to a payment processor). You'll want to maintain a diagram for each card flow that exists. Some businesses will have just one flow, but you might also have an additional flow if your website processes payment cards.

The purpose of the flow diagram is to help you understand which systems store, process, or transmit cardholder data. You can examine your actual network and decide how it fits into your card flow diagram by asking yourself:

- How is my network constructed?
- Is there one firewall at the edge of my card-processing environment?
- Is my network segmented internally?
- Does my environment have a multi-interface firewall?
- Do I have multiple firewalls?

You can then make adjustments to your network to make sure it's properly set-up.

"Don't assume that just because you were compliant for a particular control last year, you're automatically compliant this year. Requirements evolve, and emerging threats . . . emerge.

Frequently review your PCI scope and the PCI DSS to ensure you understand and properly apply the requirements."

-Trevor Hansen, QSA, CDCDP, CISSP

2 DON'T ASSUME YOU'RE COMPLIANT

PCI DSS is an evolving standard. It's designed to ensure businesses that process, store, or transmit payment card data implement security practices to prevent cardholder data theft. Since starting in 2006, the technology and business world have gone through extensive changes, and PCI DSS has needed to evolve to meet security concerns. For example, when PCI DSS was first established, merchants did not widely use mobile devices to accept card payments.

On January 1, 2015, PCI DSS 3.0 went into effect and has already been revised. Merchants have until June 30, 2016 to become compliant with PCI DSS 3.1 standards. With a continuously updated standard, you can't assume that once you are compliant with PCI DSS 3.1, you will be PCI compliant for the next couple years.

Paying attention to your PCI scope is also vital for your business. Incorrectly identifying PCI scope is a common compliance issue. The PCI DSS defines your scope as "all system components included in or connected to the cardholder data environment" (i.e., people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication). Reviewing your scope is important to know if you need to change business policies and practices.

If you change the way you process cards, or plan to make adjustments to your cardholder environment, consult with your QSA to see the impact it will have on your PCI DSS compliance.

3 UNDERSTAND YOUR RISKS

A risk assessment should occur at least annually and after significant changes in your network because it identifies threats and vulnerabilities that could negatively affect your business. Risk assessments help you avoid breaches by keeping you up-to-date with current trends, technologies, and threats. They also provide you with direction on what your next compliance efforts should be.

Addressing vulnerabilities, in particular, decreases the time an attacker can compromise the system (i.e., window of compromise). Vulnerability management plans, which identify antivirus software, patch management, coding, and control changes, are particularly helpful. This plan helps identify, classify, remediate, and lessen future instances of vulnerabilities.

Remember, just because a system is vulnerable, doesn't mean it's exploitable, or even likely to be exploited. Some vulnerabilities may require such a large number of preconditions that the chance of a successful attack occurring is virtually none. Identifying (per the guidelines of PCI DSS requirement 6) the differing levels of exploitability should help an organization prioritize the actions it will take in enhancing its IT security based on each identified vulnerability's perceived threat and risk level.

"PCI DSS requirement 12.2 requires that all entities annually perform a risk assessment that identifies critical assets, threats, and vulnerabilities. This requirement helps organizations identify, prioritize, and manage information security risks.

Understanding your risks is a step in the right direction towards protecting all of your sensitive data and achieving compliance."

-Brand Barney, QSA, CISSP, HCISPP

"To help ensure a smooth audit, perform your own internal audit during the year. During assessments, we often find that controls IT have put in place to maintain a compliant environment is not working as expected.

For example, in-scope systems may not receive critical update patches, or antivirus updates may not work on critical systems due to connection issues or misconfigurations. Internal auditing will help to ensure the controls you believe to be in place in the environment are actually working as expected."

-Michael Simpson, QSA

4 INTERNAL EXAMINATION

Onsite PCI DSS audits and forensic investigations reveal scenarios that are noncompliant with PCI DSS security requirements. However, QSA auditors don't fix every possible problem with your network; instead, they show you what is wrong with your network and ways to become PCI compliant.

PCI compliance is not an overnight task. An audit goes much more smoothly if you test your own systems throughout the year and correct any errors. Think of compliance like brushing your teeth, and an audit is similar to a dentist's checkup. A dentist can tell you if and where you have cavities or other problems, but a dentist won't be able to manage your brushing habits between check-ups.

Regularly examining and assessing your processes is vital to avoid being breached and financial consequences. If breached, you might be liable for a few or all of these fines (depending on the breach size):

- Merchant processor compromise fine: $5,000-$50,000
- Card brand compromise fees: $5,000-$500,000
- Forensic investigation: $12,000-$100,000
- Onsite QSA assessments following the breach: $20,000-$100,000
- Free credit monitoring for affected individuals: $10-30/card
- Card re-issuance penalties: $3-$10 per card
- Security updates: $15,000+
- Lawyer fees: $5,000+
- Breach notification costs: $1,000+
- Technology repairs: $2,000+
- An increase in monthly card processing fees
- Federal/municipal fines
- Legal fines

**Estimates by SecurityMetrics QSAs*

5 TALK TO YOUR ASSESSOR DURING THE YEAR

QSAs often see the full range of merchants' and service providers' struggles with PCI compliance. Auditors usually enjoy sharing their knowledge about compliance. They love to see when IT or compliance managers try their best to keep on top of compliance. If you experience a few rough patches, an auditor will gladly help.

If you can communicate with your QSA throughout the year, do it. Within a year, businesses grow; card data environments change; and PCI DSS requirements are revised. QSAs are a great resource to help you plan ahead for your audit.

Whenever there are significant changes to your environment, you should discuss potential issues or problems with your QSA to avoid the headache of reimplementation. Oftentimes they will give you advice or warning about problems they've seen in their audits.

"Communicate with your assessor throughout the year, particularly if there are any significant changes made to the environment. If there are any potential issues related to the change, you have the ability to address them upfront rather than after implementation, and while in production 1-2 months before your final report is due.

The assessor has seen a large array of different environments and might be able to provide advice or give you a heads up where others have run into problems."

-Dustin Rich, QSA, CISSP, CISA, PA-QSA

"Understand the different card data environments and be involved with business stakeholders as they look to evolve their processes so that security is 'baked' into new projects."

-Tod Ferran, QSA, CISSP

6 GET STAKEHOLDERS INVOLVED

You need to know exactly where card information is being stored, processed, or transmitted. Requirement 1.1.3 requires merchants to have a current cardholder data flow diagram. Once you know where card information flows/stores and which systems they interact with, you can easily create a card flow diagram to show how data moves within your environment.

After discovering where systems store, process, or transmit cardholder data, business stakeholders need to get involved with new procedures and with general PCI compliance.

For example, ask your staff to find other places where data might be hiding or unknowingly stored. The following areas are common areas and departments that store data:

- Error logs often store unencrypted credit card data because when an error occurs during card authentication or processing, an error log is generally created and often contains the full card data.
- Accounting departments usually have processes that store unencrypted data for financial purposes (e.g., refund processes, book balancing, charge reversals).
- Sales departments may unintentionally email or print forms containing credit card numbers.
- Marketing departments may have databases containing transaction data used for market research.
- Customer service representatives may take credit card numbers over the phone or view full card numbers, so watch for handwritten or printed card data.
- Administrative assistants may create a spreadsheet that contains a company's or an executive's credit card number for quick access when making payments.

7 KEEP DOCUMENTATION UPDATED

Documentation can be a pain for most businesses. Some may see it as another burden. However, proper documentation protects your organization, especially by keeping your security processes transparent and in order. Make sure documentation is regularly updated.

Additionally, PCI 3.0 has added many new requirements about documentation. Some of the new requirements include:

- 1.1.3 requires a cardholder data flow diagram about how cardholder data enters and leaves your network.
- 2.4 discusses creating an inventory list of all your in-scope device types and their function (e.g., POS systems and computers).
- 9.9.1 requires an up-to-date list of all devices, including physical location, serial numbers, and make/model.
- 11.1.1 involves maintaining a complete list of authorized wireless access points and the justification for each.
- 12.8.5 requires a list of all third party service providers used, PCI requirements the service providers handle, and PCI requirements the merchant is required to meet.

Most importantly, you should document when changes occur for your business policies or card data environments (e.g., security policies, software/hardware, firewall/router, diagram, etc.). These changes might alter your PCI compliance implementation.

"It's a necessary evil, but keep your documentation updated. There is nothing more enjoyable than walking into an audit and having the client provide current documentation updated to reflect all changes within the PCI DSS requirements. Throughout the duration of the year, businesses grow, card data environments change, PCI DSS requirements are amended, and those changes need to be reflected in the documentation.

This includes, but is not limited to, changes within security policies, software and hardware found within the card data environment, firewall/router configurations and rule sets, network/card flow diagrams, personnel roles and responsibilities, and the software development life cycle."

-Matt Glade, QSA, CISSP

"Often there is not a 'project lead' at a company that takes responsibility for the full compliance effort. Or, if that person exists, they are not empowered to insist on change in other groups' security postures."

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

8 ASSIGN A COMPLIANCE LEADER

PCI compliance isn't just checking yes to all the Self-Assessment Questionnaire (SAQ) questions (even though many merchants likely do this). Actual compliance requires you to implement each of the lined items.

Yes, PCI can be time-consuming and difficult at times. That's why it's best to assign one person to be responsible for PCI compliance, and this individual should be given enough resources and time to adequately handle PCI compliance. Compliance officers need to be able to challenge and correct business procedures and policies.

In preparation for an audit, compliance officers or project leads ideally have:

- An understanding of audit security jargon
- Transparent and eager attitudes to their questions and suggestions
- An already-made PCI audit checklist complete with questions to ask the auditor
- Last year's ROC printed out for them
- Documentation on how the environment is coping with recent vulnerabilities
- Talked with key stakeholders to help them understand the organization's risks
- Checked event logs regularly
- Documentation on how third party security risks are mitigated
- An understanding of PCI DSS 3.1
- An understanding of your PCI DSS scope

CONCLUSION

PCI compliance should not just be a once-a-year task to check off. In fact, you are required to maintain PCI compliance every second of every day. To help with compliance, keep contact with your QSA throughout the year, especially when you are planning any changes to your cardholder data environment.

ABOUT SECURITYMETRICS

SecurityMetrics has tested over one million payment systems for data security and compliance mandates. Our solutions combine innovative technology that streamlines validation with the personal support you need to fully understand compliance requirements. You focus on the business stuff--we've got compliance covered.

For questions about your PCI DSS compliance situation, please contact SecurityMetrics:

CONSULTING@SECURITYMETRICS.COM

801.705.5656