

SecurityMetrics Guide to



PCI DSS Compliance

A Resource for Merchants and Service
Providers to Become Compliant

[EIGHTH EDITION]

securityMETRICS®

securityMETRICS®

Looking for a
PCI compliance
solution?

Learn more at:
www.securitymetrics.com/pci

Foreword

No matter the advances in cyber security technology and despite government initiatives and regulations, attackers will continue to work to steal unprotected payment card data.

Some organizations have simple, easy-to-correct vulnerabilities that could lead to data breaches. In other instances, organizations with intricate IT defenses and processes are overridden by an employee opening a phishing email.

Our guide was specifically created to help merchants and service providers address the most problematic issues within the 12 PCI DSS requirements, showcasing auditors' best practices and IT checklists.

Our guide is not intended to be a legal brief on all aspects of PCI compliance. Rather, it approaches PCI from the perspective of a security analyst, focusing on how to protect your cardholder data. Thus, we recommend using it as a resource to help with your PCI compliance efforts.

Ultimately, our goal is to help you better protect your data from inevitable future attacks.



MATT HALBLEIB

*SecurityMetrics Audit Director
CISSP | CISA | QSA (P2PE) | PA-QSA (P2PE)*



Text copyright © 2023 SecurityMetrics

All rights reserved. No part of this publication may be reproduced in any manner whatsoever without written permission from the publisher, except in the case of quotations embodied in critical articles or reviews (or for internal educational purposes).

All inquiries should be addressed to:

SecurityMetrics
1275 West 1600 North
Orem, UT 84057

Or contact:
marketing@securitymetrics.com

Portions of this guide were adapted from material previously published on securitymetrics.com/blog and securitymetrics.com/learn.

International Standard Book Number: 978-1-7346465-7-3

The information described in this guide is presented as a reference and is not intended to replace security assessments, tests, and services performed by qualified security professionals, nor does it replace or supersede PCI DSS Requirements. Users are encouraged to consult with their companies' IT and cybersecurity professionals to determine their needs and to procure security services tailored to those needs.

Contents

Foreword	1	Requirement 7	75
INTRODUCTION	4	Requirement 8	78
How to Read This Guide	5	Requirement 9	85
PCI DSS Compliance Overview	8	Requirement 10	92
Top 10 Failing SAQ sections	10	Requirement 11	96
Understanding Your PCI DSS Responsibility	12	Requirement 12	106
SAQ Overview	16	HOW TO PREPARE FOR A DATA BREACH	114
PCI DSS Version 4.0	24	How To Prepare For A Data Breach	115
Implementing a PCI Compliant Remote Workforce Setup	35	What To Include In An Incident Response Plan	119
Forensic Perspective	37	Develop Your Incident Response Plan	123
Forensic Predictions	42	Test Your Incident Response Plan	126
PCI DSS REQUIREMENTS	44	Data Breach Prevention Tools	128
Requirement 1	45	CONCLUSION	130
Requirement 2	52	PCI DSS Budget	131
Requirement 3	57	Create A Security Culture	133
Requirement 4	63	Contributors	136
Requirement 5	67	Terms And Definitions	137
Requirement 6	70	Appendix	140



Introduction

SECTION CONTENTS

How to Read This Guide	5	PCI DSS Version 4.0	24
PCI DSS Compliance Overview	8	Implementing a PCI Compliant Remote Workforce Setup	35
Top 10 Failing SAQ sections	10	Forensic Perspective	37
Understanding Your PCI DSS Responsibility	12	Forensic Predictions	42
SAQ Overview	16		

How to Read This Guide

Whether you're a new employee with limited PCI knowledge or an experienced system administrator, the purpose of our guide is to help you secure your business and become compliant with PCI DSS requirements. We designed this document as a reference guide to address the most challenging aspects of PCI DSS compliance.

Depending on your background, job role, and your organization's needs, some sections may be more useful than others. Rather than reading our guide cover to cover, we recommend using it as a resource for your PCI compliance efforts.

NOTE:

The information described in this guide is presented as a reference and is not intended to replace security assessments, tests, and services performed by qualified security professionals. Users are encouraged to consult with their companies' IT professionals to determine their needs to procure security services tailored to those needs.



90.4%

of SecurityMetrics customers who started their SAQ went on to complete it and achieve a passing status in 2022.

The following chart displays an overview of the [PCI Security Standards Council's Prioritized Approach](#).¹ The Prioritized Approach offers organizations [a risk-based roadmap](#) to address issues on a priority basis, while also supporting organizational financial and operational planning.

The Prioritized Approach is broken down into the following six milestones (based on high-level compliance and security goals):¹

MILESTONES

- 1

Remove sensitive authentication data and limit data retention
- 2

Protect systems and networks, and be prepared to respond to a system breach
- 3

Secure payment applications
- 4

Monitor and control access to your systems
- 5

Protect stored cardholder data
- 6

Complete compliance efforts, and ensure all controls are in place

PAGE	PCI DSS REQUIREMENTS	MILESTONES					
		1	2	3	4	5	6
45	Requirement 1						
	Network Security Controls	●	●				●
	Perimeter firewalls		●				
	Personal firewalls		●				
	Properly configure firewalls		●				●
	Network segmentation		●				
52	Requirement 2						
	Apply Secure Configurations		●	●			●
	Default password weaknesses		●				
	System hardening			●			
	System configuration management		●	●			
57	Requirement 3						
	Protect Stored Account Data	●				●	●
	Encrypt cardholder data	●				●	
63	Requirement 4						
	Secure Data Over Open and Public Networks		●				●
	Stop using SSL/early TLS		●				
67	Requirement 5						
	Protect Against Malicious Software	●					●
	Regularly update your anti-malware		●				

PAGE	PCI DSS REQUIREMENTS	MILESTONES					
		1	2	3	4	5	6
70	Requirement 6 Secure Systems and Software Development		●	●			●
	Regularly update and patch systems			●			●
	Establish software development processes			●			●
	Web application firewalls			●			
75	Requirement 7 Restrict Access					●	●
	Restrict access to cardholder data and systems				●		
78	Requirement 8 Identify Users and Authenticate Access		●		●		●
	Weak passwords and usernames		●		●		
	Account Management		●		●		
	Implement multi-factor authentication		●				
85	Requirement 9 Restrict Physical Access to Cardholder Data	●	●			●	●
	Control physical access to your workplace		●			●	
	Keep track of POS terminals		●				
	Train employees early and often		●			●	
	Physical security best practices	●	●			●	

PAGE	PCI DSS REQUIREMENTS	MILESTONES					
		1	2	3	4	5	6
92	Requirement 10 Log and Monitor Access				●		●
	System logs and alerting				●		
	Establishing log management				●		
	Log management system rules				●		
96	Requirement 11 Test Security of Systems and Networks		●		●		●
	Understand your environment		●		●		
	Change and tamper detection		●				
	Vulnerability scanning vs. penetration testing		●				
	Vulnerability scanning basics		●				
	Penetration testing basics		●				
106	Requirement 12 Organizational Policies and Programs	●	●				●
	Formally document business practices		●				●
	Establish a risk assessment process	●					
	PCI DSS training best practices		●				●

PCI DSS Compliance Overview

PAYMENT SECURITY

The Payment Card Industry Data Security Standard (PCI DSS) was established in 2006 by the major card brands (e.g., Visa, MasterCard, American Express, Discover Financial Services, and JCB International).

All businesses that process, store, or transmit payment card data are required to implement the security standard to prevent cardholder data theft. The investigation of numerous credit card data compromises has confirmed that the security controls and processes required in the PCI DSS are essential to protect cardholder data.

Merchants often have a difficult time attaining (or maintaining) compliance for a variety of reasons. Many smaller merchants believe it's too technical or costly, while others simply don't believe it's effective and refuse to comply.

REQUIREMENTS OVERVIEW

REQUIREMENT 1 Install and Maintain Network Security Controls

- Install a hardware and software firewall
- Configure firewalls for your environment
- Have strict firewall rules for inbound and outbound traffic

REQUIREMENT 2 Apply Secure Configurations to All System Components

- Change default passwords
- Harden your systems
- Implement system configuration management

REQUIREMENT 3 Protect Stored Account Data

- Find where card data is held
- Craft your card flow diagram
- Encrypt stored card data

REQUIREMENT 4

Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

- Know where data is transmitted and received
- Strongly encrypt all transmitted cardholder data
- Stop using SSL and early TLS

REQUIREMENT 7

Restrict Access to System Components and Cardholder Data by Business Need to Know

- Restrict access to cardholder data
- Document who has access to the card data environment
- Establish a role-based access control system

REQUIREMENT 10

Log and Monitor All Access to System Components and Cardholder Data

- Implement logging and alerting
- Establish log management
- Create log management and monitoring system rules

REQUIREMENT 5

Protect All Systems and Networks from Malicious Software

- Create a vulnerability management plan
- Protect systems against malware and regularly update anti-virus
- Maintain an up-to-date anti-malware program

REQUIREMENT 8

Identify Users and Authenticate Access to System Components

- Use unique ID credentials for every employee
- Disable/delete inactive accounts
- Configure multi-factor authentication

REQUIREMENT 11

Test Security of Systems and Networks Regularly

- Know your environment
- Run vulnerability scans quarterly
- Conduct a penetration test

REQUIREMENT 6

Develop and Maintain Secure Systems and Software

- Consistently update your systems
- Apply all critical/high patches to systems and software
- Establish secure software development processes

REQUIREMENT 9

Restrict Physical Access to Cardholder Data

- Control physical access at your workplace
- Keep track of POS terminals
- Train your employees often

REQUIREMENT 12

Support Information Security with Organizational Policies and Programs

- Document policies and procedures for everything
- Implement a risk assessment process
- Create an incident response plan

Top 10 Failing SAQ sections

We scanned our merchant database in search of the top 10 areas where SecurityMetrics merchant customers struggle to become compliant. Starting with the least adopted requirement, these are the results:

1 SECURITY POLICY

Requirement 12.1

Establish, publish, maintain, and disseminate a security policy.

3 ANNUAL REVIEW

Requirement 12.1.1

Review the security policy at least annually and update the policy when the environment changes.

2 BREACH PLAN

Requirement 12.10.1

Create an incident response plan to be implemented in the event of system breach.

4 REQUIREMENT MANAGEMENT

Requirement 12.8.5

Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

Last year, **99.5%** of SecurityMetrics customers who finished their SAQ achieved a passing status.

5 INCIDENT RESPONSE

Requirement 12.5.3

Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

7 SERVICE PROVIDERS

Requirement 12.8.4

Maintain a program to monitor service providers' PCI DSS compliance status at least annually.

9 WRITTEN AGREEMENTS

Requirement 12.8.2

Maintain a written agreement that includes an acknowledgment that the service providers are responsible for the security of cardholder data that they possess or impact the security of the cardholder data environment.

6 AWARENESS PROGRAM

Requirement 12.6.a

Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.

8 PERSONNEL RESPONSIBILITIES

Requirement 12.4

Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

10 USAGE POLICIES

Requirement 9.9.2

Verify that the usage policies define all critical devices and personnel authorized to use the devices.

Understanding Your PCI DSS Responsibility

The PCI Council continues to update the PCI DSS. For example, the PCI Council introduced version 4.0 of the standard in March 2022.¹ You may continue to validate against version 3.2.1 of the standard until March 31, 2024, but we strongly recommend you examine the changes to version 4.0 and start planning how to implement those changes in your environment while you have time to properly test, and phase in new controls, in a disciplined manner.

PCI DSS 4.0 introduced many new controls, but the basic definition of what is in-scope has not changed. PCI scope deals with the people, processes, and technologies that must be tested and protected to become PCI compliant. An SAQ is simply a validation tool for merchants and service providers to self-evaluate their PCI DSS compliance.

If the people, process, or technology component stores, processes, or transmits cardholder data, is connected to systems that do, or could impact the security of the cardholder data environment, it's considered in scope for PCI compliance. This means that PCI requirements apply and the system components must be protected.

System components most likely in scope for your environment may include:

- Networking devices
- Servers
- Switches
- Routers
- Computing devices
- Applications

Depending on the way you process, store, and transmit payment data, there are different SAQs that you must choose to fill out. For example, if you don't have a storefront and all products are sold online through a third party, you probably qualify for SAQ A or SAQ A-EP. These different SAQ types will be further explained later in this section.

PCI DSS SCOPING AND NETWORK SEGMENTATION SUPPLEMENT

In May 2017, the PCI Security Standards Council (SSC) released a [supplemental guide for scoping and network segmentation](#).² The purpose of this guidance was to help organizations identify the systems that need to be considered in scope for PCI DSS compliance and clarify how segmentation can reduce the number of in-scope systems.

You need to understand your business environment—especially what systems are included and how those systems interact with sensitive data. You are then required to apply PCI DSS security requirements to all system components included in, connected to, or could impact the security of the cardholder data environment (CDE), which is “comprised of they system components, people, and processes that store, process, or transmit CHD or sensitive authentication data.”³

SCOPE YOUR ENVIRONMENT

When scoping your environment, start with the assumption that everything is in scope until it is verified that all necessary controls are in place and actually provide effective segmentation.

When performing your annual PCI DSS scope assessment, list and confirm all connected-to systems, which are system components that:

- Directly connect to the CDE (e.g., via internal network connectivity)
- Indirectly connect to the CDE (e.g., via connection to a jump server with CDE access)
- Impact configuration or security of the CDE (e.g., web redirection server, name resolution server)
- Provide security to the CDE (e.g., network traffic filtering, patch distribution, authentication management)
- Segment CDE systems from out-of-scope systems and networks (e.g., firewalls configured to block traffic from untrusted networks)
- Support PCI DSS requirements (e.g., time servers, audit log storage servers)

Make sure any changes to your environment are reflected in your annual scope assessment.

Without adequate network segmentation, your entire network is in scope of the PCI DSS assessment and applicable PCI requirements.

Segmentation prevents out-of-scope systems from communicating with systems in the CDE or from impacting the security of the CDE. An out-of-scope system is a system component that:

- Does **NOT** store, process, or transmit cardholder data
- Is **NOT** in the same network segment as systems that store, process, or transmit CHD
- **CANNOT** connect to any system in the CDE
- Does **NOT** meet any criteria describing connected-to or security-impacting systems

To be considered out of scope, controls must be in place to provide reasonable assurance that the out-of-scope system cannot be used to compromise an in-scope system component. Here are some examples of controls you can use:

- Firewall and/or IDS/IPS
- Physical access controls
- Logical access controls
- Multi-factor authentication
- Restricting administrative access
- Actively monitoring for suspicious network or system behavior

While not required, it's best practice to implement PCI DSS controls on out-of-scope systems to prevent them from being used for malicious purposes.

PCI DSS Scope



MATT HALBLEIB

SecurityMetrics Audit Director

CISSP | CISA | QSA (P2PE) | PA-QSA (P2PE)

To discover your PCI scope and what must be included for your PCI compliance, you need to identify anything that processes, stores, or transmits cardholder data, and then evaluate what people and systems are communicating with your systems. In May 2017, the PCI Council released an informational supplement regarding PCI scoping.² The document helps reinforce and clarify scoping points that have always been part of PCI scoping. The document can help you work through your annual scoping exercise and can lead you to discover card flows and in-scope systems that you may have previously ignored.

In my experience performing PCI audits, entities often overlook the ancillary or support types of systems when doing their own PCI scoping. For instance, call centers usually pay little attention to QA systems, which often store cardholder data in the form of call recordings. These systems are in scope for all PCI requirements!

Do not panic if you find data where it does not belong.

Simple questions can help you begin the scoping process. For example, ask yourself:

- How do you collect money?
- Why do you handle card data?
- How do you store, process, and transmit this data?

There are always processes you might not realize are in scope. For example, if you are a retail store that swipes cards, do you ever take card numbers over the phone or receive emails with card information? Are any paper orders received? Organizations often have finance, treasury, or risk groups that have post-transaction processes involving cardholder data. It is important to include these processes when determining scope.

Don't forget power outage procedures where card data is sometimes taken down manually. For example, in most call centers, we've discovered that agents are typically unaware that card data should never be written down. But when the application they use for recording cardholder data freezes, they tend to resort to typing or writing it down in a temporary location and retrieving it later for entry. These temporary locations are rarely considered in an organization's PCI compliance efforts but can lead to increased risk and should be included in your PCI scope.

Paper trails of hand-written information or photocopied payment card data can sometimes fill multiple rooms. Even if card data is ten years old, it is still in PCI scope.

If you access a web page for data entry, there's a decent chance card data can be found in temporary browser cache files. In addition, it's the website developer's responsibility to make sure websites don't generate cookies or temporary log files with sensitive data. However, you don't always have full control of your website, which is why it's important to evaluate all systems for cardholder data, even where you might not expect it to reside.

For organizations with web portals, if someone mistypes card data into an address or phone number field, it is still considered in PCI scope.

You might think your databases are set up to encrypt all cardholder data. However, servers you consider out of scope will often hold temporary files, log files, or backups with lots of unencrypted data. System administrator folders on file servers are also common culprits, as they often backup failing servers in a rush to prevent data loss without considering the PCI implications.

Usually, organizations can find ways to fix processes and delete this sensitive data, rather than add servers to their scope. A simple way to find unencrypted card data is by running a card discovery tool, such as [SecurityMetrics PANscan®](#). Organizations need to have methods to detect these mistakes and prevent or delete them. Some use a data loss prevention (DLP) solution to help them with this process.

The next step in determining your PCI scope is to find everything that can communicate with the devices you have identified. This is often the hardest part about scoping because you may not understand what can communicate to your systems. Answer the following questions:

- How do you manage your systems?
- How do you log in to them?
- How do you backup your systems?
- How do you connect to get reports?
- How do you reset passwords?
- How do you administer security controls on your systems?

If you have a server that handles cardholder data, you must always consider what else communicates with that server. Do you have a database server in some other zone you consider out of scope but is reaching that web server to pull reports and save data? Anything that can initiate a connection to an in-scope server that handles cardholder data will be in scope for compliance.

In addition, if your system in the CDE initiates a communication out to a server in another zone, that server will also be in scope. There are very few exceptions to this.



SAQ Overview

A	3.2.1	24 Questions, No Scan
	4.0	31 Questions, Vuln. Scan

Ecommerce website (third party)

- Fully outsourced card acceptance and processing
- Merchant website provides an iframe or URL that redirects a consumer to a third-party payment processor
- Merchant can't impact the security of the payment transaction

A-EP	3.2.1	191 Questions, Vuln. Scan
	4.0	151 Questions, Vuln. Scan

Ecommerce website (direct post)

- Merchant website accepts payment using direct post or transparent redirect service

B	3.2.1	41 Questions, No Scan
	4.0	27 Questions, No Scan

Processes cards via:

- Analog phone, fax, or stand-alone terminal
- Cellular phone (voice) or stand-alone terminal
- Knuckle buster/imprint machine

B-IP	3.2.1	86 Questions, Vuln. Scan
	4.0	48 Questions, Vuln. Scan

Processes cards via:

- Internet-based stand-alone terminal isolated from other devices on the network
- Cellular phone (voice) or stand-alone terminal
- Knuckle buster/imprint machine

C	3.2.1	160 Questions, Vuln. Scan
	4.0	131 Questions, Vuln. Scan

Payment application systems connected to the Internet:

- Virtual terminal (Not C-VT eligible)
- IP terminal (Not B-IP eligible)
- Mobile device (smartphone/tablet) with a card processing application or swipe device
- View or handle cardholder data via the Internet
- POS with tokenization

C-VT

3.2.1 83 Questions, No Scan
4.0 54 Questions, No Scan

Processes cards:

- One at a time via keyboard into a virtual terminal
- On an isolated network at one location
- No swipe device
- Knuckle buster/imprint machine

P2PE

3.2.1 33 Questions, No Scan
4.0 21 Questions, No Scan

Point-to-point encryption

- Validated PCI P2PE hardware payment terminal solution only
- Merchant specifies they qualify for the P2PE questionnaire

D-Merchant

3.2.1 329* Questions, Vuln. Scan
4.0 251* Questions, Vuln. Scan

Ecommerce website

- Merchant website accepts payment and does not use a direct post or transparent redirect service

Electronic storage of card data

- POS system not utilizing tokenization or P2PE
- Merchant stores card data electronically (e.g., email, e-fax, recorded calls, etc.)

D-Service Provider

3.2.1 354** Questions, Vuln. Scan
4.0 267** Questions, Vuln. Scan

Service Provider

- Handles card data on behalf of another business
- Provides managed firewalls in another entity's cardholder data environment
- Hosts a business's ecommerce environment/website or controls the flow of ecommerce data.

**Additional controls in Appendix A2*

***Additional controls in Appendix A1 and A2*

DETERMINE YOUR SAQ TYPE

How you process credit cards and handle cardholder data determines which of the 9 Self-Assessment Questionnaire (SAQ) types your business needs to fill out. Here are the different SAQ type requirements:

SAQ A

- Your company only accepts card-not-present (ecommerce or mail/telephone-order) transactions.
- All processing of cardholder data is entirely outsourced to a PCI DSS validated third-party service provider(s).
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions.
- Your company has reviewed the PCI DSS Attestation of Compliance form(s) from its third-party providers and confirmed that the providers are PCI DSS compliant for the services they are providing.
- Any cardholder data your company retains is on paper (such as printed reports or receipts), and these documents are not received electronically.
- All elements of the ecommerce payment page(s) delivered to the customer's browser originate from PCI DSS compliant providers or processors.

In summary, if your company has completely outsourced the collection and processing of cardholder data to PCI DSS-compliant third-party providers and your employees never have access to full credit card numbers, there is a strong likelihood that the SAQ A is the appropriate SAQ for your environment.

Most SAQ A merchants have an ecommerce environment that has been fully outsourced to a third-party or that either redirects the user's browser to a PCI DSS-compliant payment gateway at checkout or makes use of a third-party iFrame for payment collection.

SAQ A-EP

- Your company only accepts ecommerce transactions.
- All processing of cardholder data—with the exception of the payment page—is entirely outsourced to a PCI DSS validated third-party payment processor.
- Your ecommerce website does not receive cardholder data but controls how consumers—or their cardholder data—are redirected to a PCI DSS validated third-party payment processor.
- If the merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider).
- Each element of the payment page(s) delivered to a consumer's browser originates from your website or a PCI DSS compliant service provider(s).
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on third parties to handle all of these functions.
- Your company has confirmed that all third parties handling storage, processing, and transmission of cardholder data are PCI DSS compliant.
- Any cardholder data your company retains is on paper (e.g., printed reports, receipts), and these documents are not received electronically.

Like most SAQ A merchants, SAQ A-EP merchants have an ecommerce payment environment where the collection and processing of cardholder data have been outsourced to PCI DSS-compliant service providers. Unlike the SAQ A, SAQ A-EP websites control the flow of cardholder data to the service provider (typically using javascript or direct post methods).

If you have an ecommerce environment and you are not using a third-party iFrame or fully redirecting users to the service provider's website for payment collection but your website never receives cardholder data directly, the SAQ A-EP is likely the correct choice for your compliance documentation.

SAQ B

- Your company only uses an imprint machine and/or uses only standalone, dial-out terminals (connected via a phone line to your processor) to take your customers' payment card information.
- Standalone, dial-out terminals are not connected to any other systems within your environment.
- Standalone, dial-out terminals are not connected to the Internet.
- Your company does not transmit cardholder data over a network (either an internal network or the Internet).
- Any cardholder data your company retains is on paper (e.g., printed reports, receipts), and these documents are not received electronically.
- Your company does not store cardholder data in an electronic format.

Most SAQ B merchants receive cardholder data in person and via mail-order/telephone-order transactions and process these payments using bank-provided payment terminals that are connected to dial-up/analog phone lines. Cardholder data should never be received electronically (via email) or stored electronically. Be sure your terminals are connected to analog lines and not connected to IP networks.

SAQ B-IP

- Your business only uses standalone, PTS-approved Point of Interaction (POI) devices connected via IP to your payment processor to take your customers' payment card data.
- Standalone IP-connected POI devices are validated to the PTS POI program as listed on the PCI SSC website (excludes SCRs).
- Standalone IP-connected POI devices are not connected to any other systems within your environment.
- The only transmission of cardholder data is from PTS-approved POI devices to the payment processor.
- The POI device doesn't rely on any other device (e.g., computer, mobile phone, tablet) to connect to the payment processor.
- The business has only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically.
- Your company does not store cardholder data electronically.

Most SAQ B-IP merchants receive cardholder data in person and via mail-order/telephone-order transactions and process these payments using bank-provided terminals.

SAQ B-IP terminals are, however, connected to an IP network and transmit their data over the network instead of an analog connection. This allows for much faster processing times, but security controls must be in place to properly segment and protect payment data being transmitted over the network.

SAQ C

- Your business has a payment application system and an Internet connection on the same device and/or same local area network (LAN).
- The payment application system isn't connected to any other systems within your environment.
- The POS environment isn't connected to other locations, and any LAN is for a single location only.
- Any cardholder data your business retains is on paper (e.g., printed reports, receipts), and these documents are not received electronically.
- Your company does not store cardholder data in an electronic format.

Typical SAQ C merchants receive cardholder data in person and via mail-order/telephone-order transactions that are processed using a Point-of-Sale system that is configured to not store the full PAN (credit card number). Typical POS solutions will have multiple POS workstations/registers connected to a back-end server (the server may be hosted by a vendor/third-party). The SAQ C is designed for a simple, single-location POS deployment.

Merchants with multiple locations that are connected to the corporate office should be using the SAQ D.

SAQ C-VT

- Your company only processes payments through a virtual payment terminal accessed by an Internet-connected web browser.
- Your company's virtual payment terminal solution is provided and hosted by a PCI DSS validated third-party service provider.
- Your company accesses the PCI DSS-compliant virtual payment terminal solution through a computer that is isolated in a single location and is not connected to other locations or systems within your environment.
- Your company's computer does not have software installed that causes cardholder data to be stored.
- Your company's computer does not have any attached hardware devices that are used to capture or store cardholder data.
- Your company does not otherwise receive or transmit cardholder data electronically through any channels.
- Any cardholder data your company retains is on paper, and these documents are not received electronically.
- Your company does not store cardholder data in an electronic format.

Typically, SAQ C-VT merchants receive cardholder data in person and via mail-order/telephone-order transactions and enter the data into a PCI-compliant web-based virtual terminal using a workstation dedicated to processing payments. Workstations used to enter payment data into the third-party virtual terminal must be on an isolated network segment. Network security controls must be configured to allow only traffic required to perform this business function. All other inbound and outbound traffic to the network segment must be blocked.

SAQ P2PE

- All payment processing is through a validated PCI P2PE solution approved and listed by the PCI SSC.
- The only systems in the merchant environment that store, process, or transmit account data are the Point of Interaction (POI) devices, which are approved for use with the validated and PCI-listed P2PE solution.
- You do not otherwise receive or transmit cardholder data electronically.
- There's no legacy storage of electronic cardholder data in the environment.
- If your business stores cardholder data, this data is only in paper reports or copies of paper receipts and isn't received electronically.
- Your business has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

In order to reduce risk in a merchant payment environment and to minimize the efforts to maintain PCI DSS compliance, the PCI SSC has developed a standard for point-to-point encryption solutions. P2PE payment solutions will strongly encrypt cardholder data at the point of entry (POI device) and send the encrypted data to the P2PE solution provider for decryption and processing.

Typical SAQ P2PE merchants receive cardholder data in person and via mail-order/telephone-order transactions and process the payments using validated P2PE terminals (a list of validated P2PE solutions can be found on the [PCI Council's website](#)).⁴

SAQ D FOR MERCHANTS

SAQ D applies to merchants who don't meet the criteria for any other SAQ type. This SAQ type handles merchants who store card information electronically and do not use a P2PE certified POS system. Examples of SAQ D merchant types include:

- ecommerce merchants who accept cardholder data on their website.
- Merchants with electronic storage of cardholder data.
- Merchants that don't store cardholder data electronically but that do not meet the criteria of another SAQ type.
- Merchants with environments that might meet the criteria of another SAQ type, but that have additional PCI DSS requirements applicable to their environment.

SAQ D FOR SERVICE PROVIDERS

A service provider is a business entity that isn't a payment brand, but is directly involved in the processing, storage, or transmission of cardholder data on behalf of another organization.

Service providers can also provide services that control or could impact the security of cardholder data processed under another company's merchant account.

Examples of service providers who qualify for SAQ D include:

- A service provider that handles card data on behalf of another business.
- A service provider that provides managed firewalls in another entity's cardholder data environment.
- A service provider that hosts a business's ecommerce environment/website or controls the flow of ecommerce data.

COMBINING MULTIPLE SAQS

Some merchants will have multiple payment flows that together may not fit any SAQ type besides the SAQ D. For instance, a merchant may have an outsourced ecommerce payment channel that would fit the SAQ A but may also accept card-present transactions using an analog-connected bank terminal (SAQ B).

A merchant with multiple payment channels will likely be required to complete the SAQ D as they would not be able to affirmatively answer the qualifying criteria questions when looking at their multiple payment channels together.

Some merchant banks will allow a merchant to assess each payment channel separately with the SAQ that matches each payment channel. So, in the case of an SAQ A + SAQ B combo environment, the merchant may be able to complete an SAQ A to cover their ecommerce channel and an SAQ B to cover the card-present payment channel and provide their bank with both SAQs.

If your merchant environment consists of two or more simple payment channels, it may be worth your time to have a conversation with your merchant bank to see if you would be able to assess each payment channel separately.

PCI DATA SECURITY ESSENTIALS EVALUATION TOOL FOR SMALL MERCHANTS

The PCI council released a payment security tool—the Data Security Essentials (DSE) Evaluation Tool—to simplify security evaluation and increase security awareness for eligible small merchants. The Data Security Essentials Evaluation Tool includes 15 new categories from the PCI Council—based on payment acceptance methods—which will help smaller merchants simplify their compliance process and get the most benefit from their efforts.

“Merchants are only eligible to use a [Data Security Essentials](#) evaluation if they have been notified by their acquirer [aka their merchant bank] that it is appropriate for them to do so.”⁵

To find out more information about DSE evaluations and your possible options, contact your merchant bank.

PCI DSS

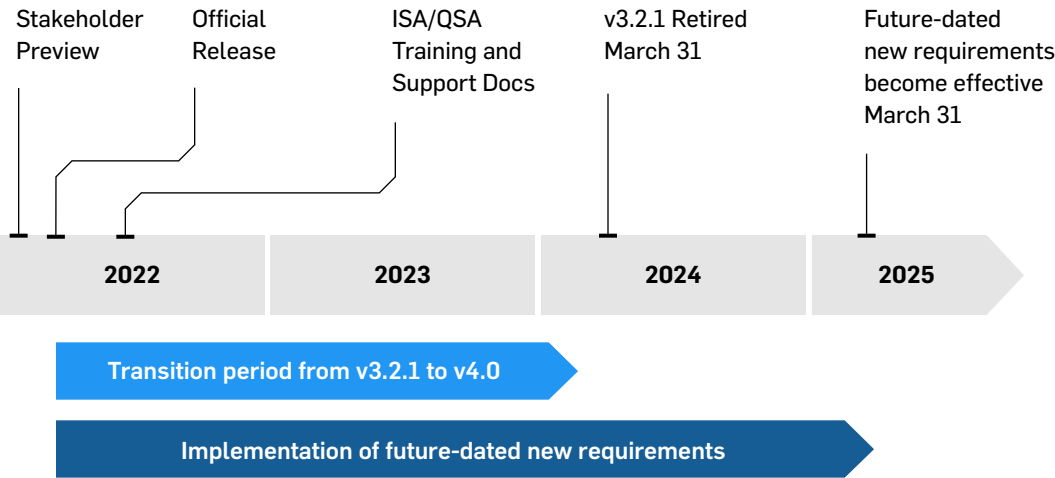
Version 4.0

PCI DSS V4.0 TRANSITION TIMELINE

The adoption of PCI DSS version 4.0 includes an overlapping sunset date for PCI DSS version 3.2.1 so that the transition between versions will be smooth.⁶ The adjacent diagram show the PCI DSS 4.0 transition timeline based on information by the PCI Council. One thing to focus on is that ample time has been provided for the transition from PCI DSS 3.2.1 to PCI DSS 4.0.

In addition, many new requirements being added to the standard are future-dated to allow new processes to be developed before any new requirements will be enforced. We have included this section to give you a quick introduction to PCI DSS 4.0 and some of the larger changes.

IMPLEMENTATION TIMELINE



THE GOAL OF PCI DSS 4.0

Why did the PCI Council make a major rewrite of the PCI DSS when it is considered to be a fairly mature standard?

There are four major reasons for the changes:

1. Ensure the standard continues to meet the security needs of the payments industry

2. Promote security as a continuous process

3. Enhance validation methods and procedures

4. Add flexibility and support of additional methodologies to achieve security

1. ENSURE THE STANDARD CONTINUES TO MEET THE SECURITY NEEDS OF THE PAYMENTS INDUSTRY

As time moves on, technology changes and so do the attack vectors of bad actors trying to compromise systems.

It is important to keep up with this changing technology. PCI DSS 4.0 addresses these changes, from scoping to cloud computing. The following table shows some of the areas of further guidance and definition. This is not an exhaustive list but will give you some ideas of what has changed.

The following information details the areas of PCI DSS 4.0 evolution:

Evolution Area	Comments
Scoping	Scoping guidance will be a more integral part of the standard itself by providing more detail on requirements for scoping validation. New requirements include tasks for organizations to verify their PCI DSS scope and some additional requirements for service providers.
Protection of Cardholder Data Transmissions	Included are continued enhancements to requirements for the protection of cardholder data in motion throughout the network.
Anti-Phishing and Social Engineering	The Council recognizes that phishing and social engineering are becoming bigger attack vectors. These are addressed in the PCI DSS 4.0 standard.
Risk Assessments	Requirements for performing risk assessments have been in PCI DSS for years; in version 4.0 these requirements expand and provide more detail for risk management as a whole. Additional requirements have been added to clarify the risk assessment process mentioned in section 12 of the standard.
Authentication	The Council aligned more closely with some industry best practices in authentication, such as addressing password length, periodic change guidelines, and multifactor authentication enhancements. These revisions to password requirements help to accommodate different authentication options.
Cloud Considerations	PCI DSS 4.0 now addresses cloud technology where it may apply in the standard. The Council has also reviewed Appendix A, which contains requirements for shared hosting providers, in order to update it with cloud technologies in mind.

2. PROMOTE SECURITY AS A CONTINUOUS PROCESS

From the beginning, PCI DSS requirements were created to help organizations develop security best practice habits that would be followed year-round, rather than only during an annual assessment period.

Many organizations have been able to make this transition to the mindset of security as a lifestyle, while others are still focused on passing an assessment and moving on.

For example, there were changes to include more gathering of validation information over a period of time to support and ensure that a continuous security process is in place.

3. ENHANCE VALIDATION METHODS AND PROCEDURES

The PCI Council has looked at validation methods and procedures to make sure they are meshing with the new PCI DSS 4.0 release.

The SAQ and AOC processes and contents were evaluated, enhanced, and released in April 2022.⁶ The new customized approach methods are not supported in current SAQ validation methods.

4. ADD FLEXIBILITY AND SUPPORT OF ADDITIONAL METHODOLOGIES TO ACHIEVE SECURITY

QSAs sometimes get asked the question, "our methods are secure; can't I meet this requirement another way?" The response had to be "We could look at defining a compensating control, but that is considered a temporary solution until you can meet the requirement the right way."

Version 4.0 of the PCI standard will try to resolve this scenario by introducing the concept of validation of a security control using a customized approach. Companies that adequately meet requirements with existing controls can continue to use these controls as a viable way to achieve compliance.

Past validation methodologies will now be known as a Defined Approach. This is essentially what we have been doing for the past 17 years. Either approach option can be used for a PCI DSS requirement and approaches can even be mixed up within a single Report on Compliance (RoC).

CUSTOMIZED APPROACH

PCI DSS 4.0 introduces the concept that not all security approaches are the same and that there may be many ways to achieve a security objective. Version 4.0 will allow customization of requirements and testing procedures in order to accommodate this.

Many companies have security solutions in place that may meet the intent of a security objective but not meet a specific requirement. This approach could let entities show how their specific solution meets the intent of the security objective and addresses the risk, and therefore provides an alternative way to meet the requirement.

This new approach will take the place of compensating controls in the PCI DSS 4.0 standard. The PCI council has stated that “Unlike compensating controls, customized validation will not require a business or technical justification for meeting the requirements using alternative methods, as the requirements will now be outcome-based.”⁷

While this new validation method may sound simple, it will most likely result in more assessment work initially for the entity in order to prepare documentation and risk assessment data for a QSA to evaluate. It will then require specialized testing procedures to be developed by the QSA and agreed upon by the entity.

The customized approach will not be for everyone and will be most suited for entities with mature security and risk assessment processes in place.

The custom process provides the advantage of defining a more permanent solution for compliance validation of specialized security controls. This is different from previous temporary compensating controls in earlier versions of the standard, where you had to document a justification for the control with a business or technical constraint.

Customized Approach Milestones:

The customized approach offers more validation flexibility, but it's not ideal for everyone. The following figure illustrates where responsibilities lie when using the customized approach:

THE ENTITY

Implements control(s) that meets the intent of the PCI DSS Requirement

Provides documentation that describes the customized implementation

- The who, what, where, when, and how of the controls
- Evidence to prove the controls meet the stated intent
- Evidence of how controls are maintained, and effectiveness is assured

THE ASSESSOR

Plans and conducts the assessment

- Reviews information provided by the entity
- Derives testing procedures based on information provided
- Documents details of testing procedures and results of testing in the ROC

Relying on a security implementation you already have in place may save on new capital expenses, but it will require more work on your part. You will need to thoroughly document, test, and conduct risk analysis efforts to present to your QSA. The QSA then has to review your information to develop custom testing procedures—a process that will require more reporting from the entity.

Therefore, an assessment using the Customized Approach will likely require more resources than an assessment using the defined approach, but it may be a more cost effective method when all aspects are considered. Be sure to look for a QSA with the depth and years of experience necessary to validate custom controls and develop appropriate testing procedures.

The Customized Approach method shouldn't be a way to disengage from your assessment. Rather, utilizing the Customized Approach should encourage working closely with your QSA.



CUSTOMIZED APPROACH AND RISK ASSESSMENTS

As mentioned in the previous section, the Customized Approach is now available. However, before jumping right in, larger organizations and risk assessment teams may want to look at the Defined Approach and Customized Approach so that they understand the differences between the two and can make the right decisions for their organization.

A lot of people are excited about the Customized Approach because it sounds easier to get compliant. In reality, it's going to be more complicated than it sounds. The Customized Approach requires a lot of work and effort to define what the actual requirements are and how to measure the requirements.

One of the biggest adjustments to PCI 4.0 is the increased use of risk assessments within the Customized and Defined Approaches. Risk assessments for a Customized Approach are a big part of the new standard. Instead of being a simple and quick process, organizations will need to follow a very structured formalized risk assessment.

In the past, people weren't certain about what risk assessments were or the associated requirements. We'd often ask questions like "have you had a meeting, or have you written a document, or have you done something that shows that you've thought about the risks in your system?"

Now, the expectation is that if you make a change in your environment (e.g., adding a new firewall), you need to do a risk assessment on that change.

If you don't have a lot of experience with a formal risk assessment, or don't have a risk department as part of your company, you may need initial help from a third party to get you going and learn how to do these things.

Formal risk assessments may not seem like a big change based on some of the other future dated requirements that have been added to the standard, but this change in PCI DSS 4.0 may result in additional effort in the transition process.

KEY PCI DSS 4.0 REQUIREMENT UPDATES

Here's a quick overview of some key new requirement changes in each section of PCI DSS 4.0 effective [March 31, 2025](#):

Requirement 1

There were no significant changes.

Requirement 2

There were no significant changes.

Requirement 3

3.2.1 *(March 31, 2025)*

In the past, if you stored sensitive authentication data before authorization, it was recommended that you should try to encrypt or protect it, but it wasn't required. Now, it is required.

3.3.3 *(March 31, 2025)*

Issuers now must encrypt the sensitive authentication data that they may be storing. This may not be a big deal for most issuers at this point, but it may be difficult for some legacy systems where encryption software is not readily available.

3.4.2 *(March 31, 2025)*

If you're using remote access technology to access the cardholder data environment (CDE), then you must prevent the copy and relocation of primary account number (PAN) data. This has been mentioned before, but now it will be a requirement.

addressing this process, but now it needs to be enforced by some technology. There may be settings in your remote access software that have ways of preventing access to certain functions. Depending on what resources you have and your current processes, this requirement may or may not be difficult to implement.

3.5.1.1 *(March 31, 2025)*

PCI DSS 4.0 also changes the security required on hashing functionality if your system is using a hash method for protecting card data.

Organizations will need to use a keyed cryptographic hash method, which is different from most common hash algorithms in use. So you may need to change your hashing algorithm to something like HMAC, CMAC, or GMAC, with an effective cryptographic strength of at least 128-bits. A code change of this kind could take

some effort so you may want to focus on this earlier rather than later.

3.5.1.2 *(March 31, 2025)*

This requirement discusses the removal of disk-level encryption as an option to protect card data. Now it can only be used for removable media (e.g., a USB drive, an external SSD). You can't use it anymore on your computer's hard drive or any kind of non-removable media. If you're using disk-level encryption for protection, you will need to make some changes.

Requirement 4

4.2.1 *(March 31, 2025)*

A new requirement in this section will be to carefully document, track, and inventory SSL and TLS certificates in use for the transmission of sensitive data across public networks. Increased tracking will help ensure the certificates' continued strength and validity. So, it's just a new process and tracking that needs to be implemented.

Requirement 5

5.3.3 (March 31, 2025)

Organizations will need to scan removable media used in the CDE. Since most antivirus solutions do this or have the capability, it may just require some configuration setting changes. Review the capabilities of the malware solution you are using to see if they have these capabilities.

5.4.1 (March 31, 2025)

One of the bigger changes is that a requirement to have automatic process mechanisms in place to detect and protect personnel against email phishing attacks has been added.

If you're doing your email in house, you may or may not have had all the controls in place for this yet. If you've outsourced emails, confirm with your provider and see what sort of protections they have against phishing attacks.

Requirement 6

6.4.2 (March 31, 2025)

In PCI DSS 3.2.1, a web application firewall or a process to do code reviews was required to protect web applications developed by a company. In March 2025, organizations will need to have a web application firewall in place for any web applications exposed to the Internet.

This standard has been a long time coming and shouldn't be surprising. There are many solutions, including cloud-based solutions, that can help with this requirement.

6.4.3 (March 31, 2025)

To reduce the possibility of malicious scripts making it onto payment pages, organizations need an inventory of all the known scripts used on those pages.

This inventory must be documented and tracked to ensure that all the scripts used are authorized, and that the integrity has been validated. Review the guidance column for further information on this requirement.

Requirement 7

7.2.4, 7.2.5, 7.2.5.1 (March 31, 2025)

Not much has changed in this section. It's the basic, role-based access control requirements, and most of the changes are just tightening account reviews and processes around reviews for systems, users, and applications.

Requirement 8

8.3.6 (March 31, 2025)

To strengthen passwords, the minimum length of passwords is moving from 7 to 12 alpha and numeric characters.

Depending on your applications, this could be a simple fix or it may require some code changes. So, start checking now to see if there are any systems in use in your CDE that would have difficulty with this future dated requirement.

8.3.10.1 (March 31, 2025)

Another change in section eight around passwords pertains to service providers. Customers of service providers will now have to change their passwords every 90 days if you're using just a password for authentication (i.e., you are not using a multi-factor authentication).

8.4.2 *(March 31, 2025)*

Multi-factor authentication will be required for all access to the CDE, not just from external locations. So this would apply to internal administrative access to servers, firewalls, networking gear, etc.

8.5.1 *(March 31, 2025)*

PCI DSS 4.0 adds a new detail to MFA requirements that might be a bit tricky. Success of all the factors has to happen before authentication, and it can't be known from the process which factor has failed.

Presently, most systems ask for a username and password (i.e., something you know) and only move on to the second factor if you have the correct username/password. This will no longer be allowed.

Both factors will have to be presented and entered without revealing any information about which factor might have been wrong if authentication fails.

8.6.2 *(March 31, 2025)*

All application and system passwords that could be used for interactive login have additional approval and tracking controls on their use, and can no longer reside in a script or a file.

Requirement 9

There were no significant changes.

Requirement 10

10.4.1.1 *(March 31, 2025)*

Organizations can no longer review their logs manually.

Few, if any, companies are manually reviewing logs anymore as it's just too much data to effectively review manually. There are many log review tools out there so it shouldn't be difficult to implement a solution. Manual review of logs is time-consuming and easy to do poorly, so this is a good change.

10.7.2 *(March 31, 2025)*

All organizations must now detect, alert, and promptly address failures of critical security control systems. This used to be only required for service providers, but has now been extended to everyone.

This means that if you had a firewall or IDS system that went down for some reason, you would have to detect it, generate an alert, and respond to that alert. This update will require additional procedures for merchants to implement. We recommend that you start now to look for solutions.

Requirement 11

11.3.1.2 *(March 31, 2025)*

Internal vulnerability scanning must now be authenticated. This means that it's not just a scan of ports and services; now, if a service is exposed that requires a credential to access it (e.g., a web app), you need to use those credentials to gain access and test the authenticated port or service.

An important part of this new requirement will be that the credentials used by the vulnerability assessment (VA) scanner must be entered into the system and stored securely. This will have to be a feature of the VA scanning solution and should be something you check with your vendor carefully on.

11.5.1.1 *(March 31, 2025)*

Another requirement change was on IDS/IPS, so that systems detect and alert on any covert malware communication channels that are being used (i.e., DNS tunneling). This may represent a change to the IDS/IPS system that you are currently using.

11.6.1 *(March 31, 2025)*

One of the biggest things in section eleven was the addition of a requirement to implement a change and tamper detection mechanism for any payment pages. This requirement addition is a direct result of the increase in ecommerce skimming compromises seen on payment pages in recent years.

Before March 31, 2025, companies will have to deploy a solution that will detect changes to those pages (e.g., script additions, changes to known script and code).

This is a great addition to the standard and is absolutely needed for ecommerce websites.

Requirement 12

12.5.2

(Immediately Effective for 4.0 Assessments)

An annual scoping of your card data environment was mentioned in the initial discussion section of previous versions of PCI DSS, but now the Council has moved that into the requirements matrix under section 12 and made it a trackable requirement effective immediately for version 4.0.

So a documented scoping exercise will have to be done by merchants annually, or after any significant changes to the in-scope environment (e.g., people, systems, processes).

12.5.2.1 *(March 31, 2025)*

New for service providers will be a future dated requirement to perform this scoping exercise at least every six months and after any organizational changes to the company.

12.6.2 *(March 31, 2025)*

Organizations will need to enforce a more formal Security Awareness Program, where before you could get by with some basic security training.

Organizations will need to document and update their Security Awareness Program at least once every 12 months and as needed to address any new threats and vulnerabilities that may impact the security of their CDE or information provided to personnel about their role in protecting cardholder data.

12.6.3.1 *(March 31, 2025)*

The standard now expects a security training program to discuss specific threats and vulnerabilities in your environment, as well as acceptable use of end-user technologies.

For example, if phishing is a big deal for your environment, then you need to address phishing in your training. The training program will also need to be reviewed and updated at least annually.

12.10.7 *(March 31, 2025)*

Incident response procedures will need to be initiated if stored primary account numbers (PAN) is detected anywhere it is not expected. This means that you are always on the watch for new or errant processes creating repositories of stored PAN outside of expected boundaries.

Periodic review of processes dealing with card data and running a good data discovery tool will be needed to fully say you have satisfied this future dated requirement.

TAKEAWAYS

What are the most important things to focus on right now?

First, read the PCI DSS version 4.0 standard and get familiar with the bigger changes that could impact your compliance process. Then start formulating your plans right now to implement changes for version 4.0. There is plenty of time, so start early and you will not have problems making the transition. During this planning process don't forget to keep working hard to keep your current efforts going to be compliant to PCI DSS version 3.2.1.

Second, start thinking about how you are conducting your risk assessments. More formal risk assessment processes are required in version 4.0 and most organizations will have to add processes and gain skills to do this correctly. Start researching formal risk assessments and refer to the industry standards out there like NIST 800-30 and OCTAVE to begin getting familiar with them. It may be a good idea to consult with a QSA as you develop these processes.

Finally, don't wait until 2024 to begin switching over to PCI DSS 4.0. Spread your efforts across the next couple of years and you will be just fine with the new requirements.

PCI DSS 4.0 SUMMARY

As a reminder, PCI DSS version 4.0 may seem daunting, but it is actually an improved way to counteract the techniques used by threat actors. Preparing for compliance to version 4.0 is straightforward if you are already working towards or maintaining compliance to PCI DSS 3.2.1.

Implementing a PCI Compliant Remote Workforce Setup

It is increasingly common for companies to allow employees to work from home. It is important to remember that if cardholder data is processed, transmitted, or stored by employees working from home, their home environment will be part of the organization's PCI scope.



THE SCOPE OF THE REMOTE WORK CDE

When scoping a work-from-home implementation where employees will be collecting or processing cardholder data, begin by mapping out the flow of cardholder data.

Questions to answer:

- How is data being received by the employees (e.g., over the phone, fax, Internet communications)?
- Once this data is received, how are employees processing the data?
- What devices and network segments are involved in the transmission of cardholder data?
- Is cardholder data being stored electronically or on paper?
- What type of voice communication channels are involved?
- If cardholder data is received over the phone, are calls being recorded?

Realize that any system involved in the storage, processing, or transmission of cardholder data is in-scope for your environment, as is any system that can affect the security of these devices.

EXTENDING THE EXISTING CDE

Many organizations will already have an existing CDE with mature controls designed to protect customer data. When implementing a work-from-home scenario, attempt to leverage the tools and security controls that exist in the corporate environment.

Assume that the employee's home network and computer are not a secure option for processing payments. You can maintain the security stance of your CDE by extending your CDE network via VPN connectivity and providing company-owned mobile devices that have been hardened and can be managed remotely. Also, keep in mind that split tunneling should be disabled in order to maintain proper network segmentation.

Most enterprise phone deployments have moved to Voice over IP (VoIP). VoIP offers great flexibility that can also be leveraged in a work-from-home scenario. If your CDE includes telephone-order options, send VoIP endpoints home with your employees that will extend your VoIP system over an encrypted connection (such as a VPN).

For more information on protecting voice communications, see the [PCI SSC's guidance on Protecting Telephone-based Payment Card Data](#).⁸

RISK REDUCTION STRATEGIES

If you are unable to extend your CDE network to remote locations, implementing P2PE may be a good option to reduce both the cost of compliance and the risk to your customer's payment data.

There are a variety of P2PE devices that can be used to input cardholder data. Some of these devices are standalone terminals, while others can be used as a USB connected keypad. Implementing a [P2PE endpoint](#) may allow you to keep the employees' computer and network out of scope for your environment.

Forensic Perspective

INTRODUCTION

SecurityMetrics Payment Card Industry Forensic Investigators (PFI)s* thoroughly analyze the point-of-sale (POS) or ecommerce environments of organizations that suspect a payment card data compromise.

Through a forensic examination of the in-scope computer systems related to the processing of customer payment card information, data acquired from the breach site can reveal when and how the breach occurred, contributing vulnerabilities, and aspects of the IT environment out of compliance with the PCI DSS.

SecurityMetrics Forensic Investigators have witnessed the rise and fall of popular attack trends over 20 consecutive years.

Comparing recent forensic trends to previous years, SecurityMetrics' Forensic Investigators conducted more investigations of ecommerce environments than of point-of-sale (POS) environments.

The following section will further discuss predicted forensic trends..

**SecurityMetrics PFIs are Qualified Security Assessors, but do not perform a complete QSA audit of each PCI requirement during a PCI forensic investigation. PCI DSS requirement data is analyzed to the extent observed throughout the course of an investigation.*

Never Have
a False Sense
of Security.™

Learn More About
SecurityMetrics
PCI DSS Audits.

[Learn More](#)

ECOMMERCE SECURITY TRENDS

Findings From SecurityMetrics' Ecommerce Security Service

SecurityMetrics Shopping Cart Inspect helps businesses detect if their Shopping Cart has been breached.

With the help of Shopping Cart Inspect, SecurityMetrics Forensic Analysts review businesses' rendered webpage code on their shopping cart URL to collect evidence of a skimming attack.

68.3%

of discovered issues
were suspicious.

68.3%



92.4%

92.4% of Shopping Cart Inspect reviews identified malicious, suspicious, and/or concerning issues on researched ecommerce sites.

On average, inspected websites had 2.44 issues discovered.

Those issues include the following classifications:

- **Malicious:** Evidence of card data being stolen. (*Highest threat level*)
- **Suspicious:** Identified issues increase the probability of a potential exploit. (*Medium threat level*)
- **Concerning:** Unlikely method of being breached, but identified issues could lead to a potential exploit. (*Low threat level*)

3.7%

of issues were malicious.

of issues were suspicious.

28%

of issues were concerning.

TOP 5 MALICIOUS ISSUES FOUND

1. **Malicious Double Checkout**
Double post of credit card data returning to alternate checkout page on merchant's server.
2. **Malicious Post**
A script is running with a post of data to a known bad site.
3. **Malicious Javascript**
Javascript appears to be acting in a malicious manner, such as harvesting credit cards or other sensitive data.
4. **Form Jacking**
Authorized payment webform is being replaced by a counterfeit.
5. **Directory Browsing Enabled**
Directory Browsing is enabled on the web pages analyzed.

TOP 5 SUSPICIOUS ISSUES FOUND

1. **Javascript issue**
Out-of-date JavaScripts can lead to vulnerabilities available for future malicious attacks.
2. **Ads/Business Intelligence**
Advertising/Analytics content is being pulled into the pages being reviewed in the checkout environment. This can be a source of intermittent card/data loss due to drive-by malvertising.
3. **Out-of-date CMS - Suspicious**
Out-of-date web components. Unpatched or un-updated software is a leading cause of sites losing sensitive data.
4. **Configuration Issue**
Missing required web server security headers.
5. **Suspicious double checkout**
Double post of credit card data returning merchant's checkout page on the server. This practice could impact security of the site and should be reviewed for business need.





[LEARN MORE](#)

Detect eskimming
on your website.

TOP 5 CONCERNING ISSUES FOUND

1. **Configuration Vulnerability**

A configuration item with a website or web server is not following best security practices.

2. **Checkout Configuration Issue**

The implementation of certain aspects of the checkout process may not follow best security practices and could leave merchants vulnerable to certain types of attacks.

3. **Mixed HTTP/HTTPS**

Content called via HTTP in an HTTPS environment, breaking strict SSL/TLS protocol. In severe cases, this can be exploited by bad actors to view privileged content.

4. **HTTP Header Issue**

Improperly configured HTTP headers can provide attackers with specific information about your web server setup, such as vulnerable software versions.

5. **SPAM Watch**

A domain has been flagged by the SPAM community, which could be using the email server to transmit malicious communications by bad actors.

Forensic Predictions

PREDICTION 1

INCREASED PHISHING SOPHISTICATION

Last year, a major company was breached about every week, let alone the numerous cases of small businesses falling for phishing. Some of these breaches even came from teenagers tricking these large organizations by utilizing sophisticated phishing attacks.

For example, one recent phishing example we've seen become more relevant is phishing emails sending requests through electronic signature tools. Once you click on what you believe is a form to fill out or sign, you are taken to a blank image. That blank image has malware embedded into it, enabling malicious attackers to gain control of the network.

Even if these applications make changes to stop these attack vectors, bad actors will pivot and try other methods to send out phishing emails, such as utilizing AI technology to help craft phishing emails.

Another example is of bad guys targeting call centers, where they impersonate a customer trying to set up an account and after being unsuccessful send a screenshot to a support agent, only for the screenshot to contain malware that gets uploaded to the support agent's computer and the corporate network.

Another trend that's increased is SMS phishing or smishing. This is where your text messages are being used against you, with attackers trying to get access to automatic two-factor authentication codes that come up in text messages. But if your phone has been compromised via one of these previous methods, attackers will be able to access the code before you do.



PREDICTION 2

MOBILE ATTACK SURFACE INCREASES

Mobile attack surfaces will continue to increase. There are a plethora of phone apps, from banking apps to retail apps to social apps, all of which are capable of web view capability. If an attacker can launch and hijack the JavaScript, they can instigate a numbers of attacks. For instance, if it pulls up a URL, they can conduct overlay attacks, where they mimic your bank's login portal or create a form that goes right over the top of your website's checkout form, allowing them to steal your customers' sensitive information.

Much of this issue is the attack surface itself, where you have all of these apps but then don't have a method to filter or detect spam to either be turned on or natively enabled.

You also have incoming messages being displayed regardless of the content on the mobile phones.

You need to focus on cybersecurity due diligence and your user security awareness because even with all the technical controls in place, these phones can be an easy gateway into your business security. Previously, these mobile browsers were put in a sandbox, with it being difficult for third party coding to be injected into these sandboxed apps.

But now with web view, these attackers will continue to target the web view browser.

We recommend that if you don't need an app on your phone, get rid of it. If you do keep an app on your phone, you need to update it regularly.

PREDICTION 3

DEV ENVIRONMENT RISK

Many recent breaches have actually come from the development environment. This is because developers are looking for ways to speed up production, testing, and deployment, looking for more methods to automate code. Developers are likely dealing with increased pressure to launch new products to the market as fast as possible. Often this speed comes at a cost of security.

Cyber hygiene and a robust security posture has never been more important. The dev attack surface is only going to grow, and bad guys are starting to figure this out. Recently, we've seen attackers looking for backdoors that will allow them access to the dev environment.

Beyond backdoor vulnerabilities and active former DevOps accounts and credentials, third parties or contractors open up security vulnerabilities to organizations. For example, impersonation attacks that compromise dev tools and code libraries will continue to be a huge security issue, such as with clipper malware, which hijacks a user's clipboard data.



PCI DSS Requirements

SECTION CONTENTS

Requirement 1	45	Requirement 7	75
Requirement 2	52	Requirement 8	78
Requirement 3	57	Requirement 9	85
Requirement 4	63	Requirement 10	92
Requirement 5	67	Requirement 11	96
Requirement 6	70	Requirement 12	106

Requirement 1

Install and Maintain Network Security Controls

Network firewalls are vital for your security. A firewall's purpose is to control network traffic into and out of your environment. Simply installing a firewall on your organization's network perimeter doesn't make you secure; it must be configured properly.

PERIMETER FIREWALLS

A properly configured business-grade perimeter firewall acts as the first line of defense and blocks unwanted network access. While these are often physical devices, they can be offered as services in cloud environments, where they are often referred to as network security groups.

A firewall is typically installed at the perimeter of an organization's network to protect internal networks from untrusted networks, such as the Internet, often by restricting the types of network traffic permitted into the organization's network and the locations from where the traffic originates. Perimeter firewalls can also be used inside an environment to create isolated network segments. Higher security internal network segments are created to limit access to sensitive data from less secure networks.

PCI DSS requires a firewall between any systems that store sensitive data and any systems on your network that can be accessed from the Internet (generally known as the DMZ).

PERIMETER FIREWALL PROS

- Most robust security option
- Protects an entire network
- Can segment internal parts of a network

PERIMETER FIREWALL CONS

- Rules need to be carefully documented
- Difficult to configure properly
- Needs to be maintained and reviewed regularly

PERSONAL FIREWALLS

Many personal computers come with pre-installed software firewalls. This feature must be enabled and configured for any laptop computers that commonly connect to sensitive data networks and are also used to connect to the Internet when outside the network.

Personal firewalls protect the system they are on, while perimeter firewalls protect entire networks. A personal firewall can be configured to permit more or less network traffic, depending on the network to which it is attached. For example, it might allow more types of network traffic when the machine is on the company network, but limit it when on public Wi-Fi.

PERSONAL FIREWALLS PROS

- Protects mobile workers when outside the corporate network
- Easier to maintain and control
- Inexpensive

PERSONAL FIREWALLS CONS

- Should not replace perimeter firewalls for network segmentation
- Doesn't protect an entire network
- Fewer security options

PROPERLY CONFIGURE FIREWALLS

A common mistake regarding firewalls is assuming they are a plug-and-play technology. After initial installation, additional effort is almost always necessary to restrict access and protect the CDE.

The end goal of firewall implementation is to prevent potentially harmful traffic from the Internet and other untrusted networks from accessing valuable confidential data, and to prevent data from being exfiltrated by malicious actors. In ecommerce applications, a firewall should be used to limit traffic to essential services needed for a functioning CDE. By identifying sensitive systems and isolating them through the proper use of firewalls (e.g., network segmentation), merchants can more precisely control what type of access is allowed in and out of these zones, and more easily protect payment data.

In a data breach investigation conducted by SecurityMetrics Forensic Investigators, an organization had a sophisticated security and IT system. However, amongst 300 pages of firewall rules (with about 100 rules on every page), two incorrectly written firewall rules left the entire network exposed. It was through this vulnerability that the attacker accessed their network and stole sensitive data.

FIREWALL CONFIGURATION BEST PRACTICES

1. **Create Firewall Configuration Standards:** Before implementing firewall settings and rules on the hardware, carefully document settings and procedures such as hardware security settings, port/service rules needed for business, and business justification for each rule. Make sure you consider both inbound and outbound traffic.
2. **Trust But Verify:** After implementing firewall rules/settings, test the firewall from both external and internal perspectives to confirm settings are correct using penetration test, vulnerability scans, and other automated and manual tools and techniques.
3. **Limit Outbound Traffic:** Often, we worry too much about blocking inbound ports/services and forget that outbound traffic from inside the network should be limited as well. This limits malicious actors' paths for exfiltrating data.
4. **Personal Firewalls:** Configure personal firewalls on mobile computing platforms to limit riskier types of network traffic when on unsecured networks.
5. **Management:** Manage the firewall itself from within your network. Disable external management services unless they're part of a secure managed firewall infrastructure.

Never Have
a False Sense
of Security.™

Learn More About
SecurityMetrics
PCI DSS Audits.

[Learn More](#)

NETWORK SEGMENTATION

Merchants often set up flat networks, meaning everything inside the network can connect to everything else. They may have one firewall at the edge of their network, but that's it. There's no internal segmentation, making it a *flat network*.

Flat networks make security difficult because if an attacker gets inside, they have access to everything.

Initial intrusion in many of recent investigated data breaches began in areas of an organization's network that shouldn't have given the attacker access to the CDE. For example, since the organization's network was configured as a flat network, it was not difficult for the attacker(s) to migrate from the point of entry (e.g., employee laptop, workstation) to the CDE or other sensitive systems.

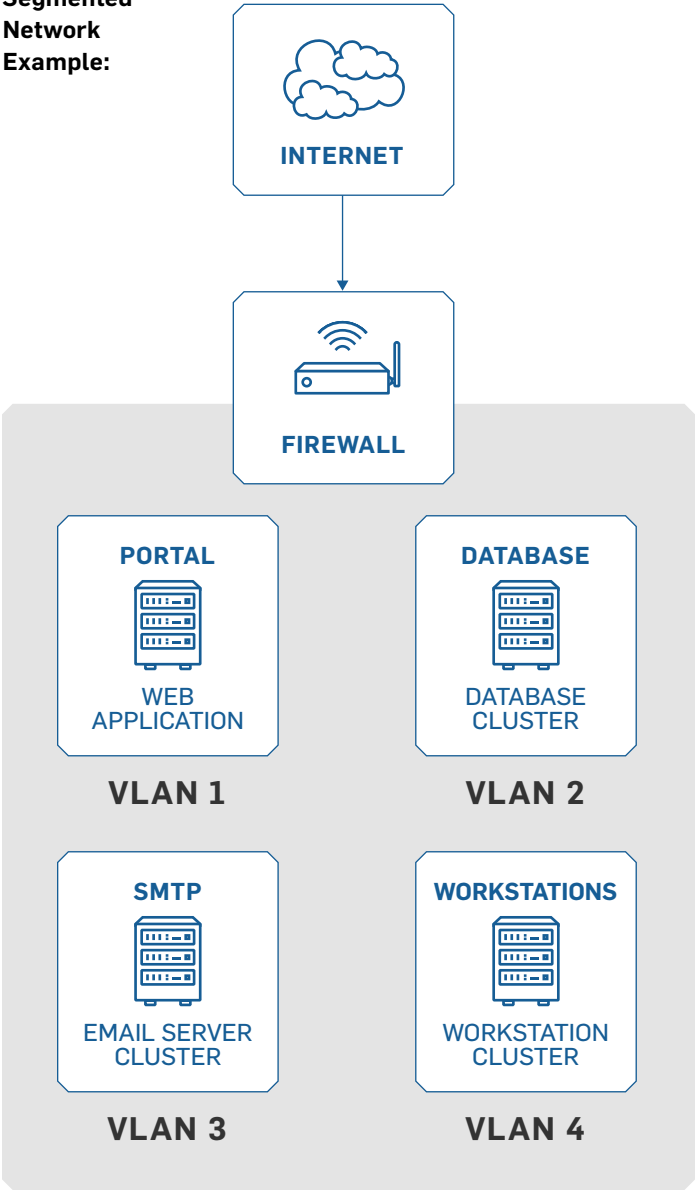
Firewalls can be used to segment an organization's network. When businesses create a secure payment zone—firewalled off from the rest of the day-to-day business traffic—they can better ensure their CDE only communicates with known and trusted sources. This limits the size of the CDE and potentially lowers your PCI scope.

For example, install and configure a multi-interface firewall at the edge of your network. From there, create one interface on the firewall dedicated just to the systems that store, process, and transmit cardholder data. If that interface doesn't allow any other traffic in or out of any out-of-scope zones, this is proper network segmentation.

Segmentation is not required for you to be compliant with PCI DSS. However, if you're looking for a way to reduce cost, effort, and time, you may want to consider segmentation.

Segmentation can be tricky, especially for those without a technical security background. Consider having a security professional double-check your segmentation work by performing regular, third-party segmentation checks.

**Segmented
Network
Example:**



TEST AND MONITOR CONFIGURATION

Rules and environments change over time, no matter the size of your organization. Firewall rules should be reviewed (and revised when necessary) over the course of a few months whenever your environment undergoes a significant change and at least every six months.

Requirement 1: Establish Secure Firewall Rules



JEN STONE

SecurityMetrics Senior Security Analyst
CISSP | CISA | QSA | CCSFP | CHQP

Large environments typically have firewalls in place, but they might not be business-grade. Make sure to choose firewalls that support the necessary configuration options to protect critical systems and provide segmentation between the CDE and other internal and external networks specific to your organization.

Smaller organizations sometimes struggle to understand firewalls, not having the necessary in-house expertise to configure and manage them correctly and securely. If this is the case, contract a PCI-validated third-party service provider to provide assistance, rather than simply deploying a firewall's default configuration and hoping for the best.

It may seem obvious, but leave as few holes as possible in your firewall.

“Firewalls are a first line of defense, so pay special attention to the logs and alerts firewalls generate.”

It's best to start by having a *block everything* mentality, and then add exceptions as needed. PCI DSS requires you to document a valid business justification for any communication allowed to or from the CDE. Spend the time to identify the specific source and destination addresses your systems need to communicate with for a given service or protocol. Don't just allow all access to the Internet because it's easier. Along the same lines, if you or any third parties remotely support your environment, limit that inbound access to specific sources and protocols.

Often, the volume of log data can be overwhelming, so some merchants turn logging off or send alert messages directly to the junk bin. It's important (and required) to review firewall logs daily to identify patterns and activity that indicate attempts to breach security. There are many good software packages available to help you deal with the volume of log data and automate alerts, or you may choose to engage the help of a service provider.

For requirement 1, remember the following:

- Start with a “block everything” mentality, only opening up what is necessary.
- Pay attention to what logs tell you.
- Review firewall configurations frequently and adjust as necessary.

REQUIREMENT 1 IT CHECKLIST

Firewall Implementation And Review

Assigned to:_____

Assignment date:_____

Things You Will Need To Have:

- Firewall(s)
- “Deny All” rule for all other inbound and outbound traffic
- Stateful inspection/dynamic packet filtering
- Documented business justification for each port or protocol allowed through the firewall

Things You Will Need To Do:

- Limit traffic into the CDE to that which is necessary
- Position firewall(s) to prohibit direct inbound and outbound traffic from the CDE
- Create secure zone(s) for any card data storage, which must be separate from DMZ
- Explicitly authorize outbound connections from the CDE
- Document all firewall policies and procedures
- Review firewall logs daily for potential breach activity

Things You May Need To Do:

- Install a firewall between wireless networks and the CDE (wireless only)

NOTES

Requirement 2

Apply Secure Configurations to All System Components

DEFAULT PASSWORD WEAKNESSES

Out-of-the-box devices, such as routers or POS systems, often come with factory settings like default usernames and passwords. Defaults make device installation and support easier, but they also mean every model originates with the same username and password. Default passwords are easy to guess, and many are published online.

Businesses are often unaware that default settings are used in their environment, due to third-party installation.

In one [SecurityMetrics forensic investigation](#), it was discovered that a third-party IT vendor purposely left POS system default passwords in place to facilitate easier future system maintenance. Default passwords might make it easier for IT vendors to support a system without learning new passwords each time, but convenience is never a valid reason to forego security, nor will it reduce liability.

When defaults aren't changed, it provides attackers an easy gateway into a system, which is why changing vendor defaults on every system with exposure to your CDE is so vital.

Passwords must be changed every 90 days and contain at least seven characters, including numbers and letters.

Passwords that fall short of these criteria can usually be broken in a short time using readily available password-cracking tools.

SYSTEM HARDENING

Any system used in your CDE needs to be hardened before it goes into production. Every application, service, driver, feature, and setting installed on a system may introduce vulnerabilities. The goal of hardening a system is to remove unnecessary functionality and configure what is left in a secure manner.

Here are some recommended resources for system hardening:

- Center for Internet Security ([CIS](#))
- International Organization for Standardization ([ISO](#))
- SysAdmin Audit Network Security ([SANS](#)) Institute
- National Institute of Standards Technology ([NIST](#))

SYSTEM CONFIGURATION MANAGEMENT

Consistency is key when trying to maintain a secure environment. Once system hardening standards and settings have been defined and documented, it is critical that they are applied to all systems in the environment in a consistent manner. Once each system and device in the environment has been appropriately configured, you still have work to do.

Make sure someone is responsible for keeping the inventory current and based on what is actually in use.

This way, applications and systems that are not approved for use in the CDE can be discovered and addressed.

Many organizations, especially larger ones, turn to one of the many system management software packages on the market to assist in gathering and maintaining this inventory. These applications can scan and report on hardware and software used in a network and also detect when new devices are brought online. These tools are often able to enforce configuration and hardening options, alerting administrators when a system isn't compliant with your internal standard, or even re-applying standard configurations when changes are detected.



Requirement 2: System Configuration



JEN STONE

SecurityMetrics Senior Security Analyst
CISSP | CISA | QSA | CCSFP | CHQP

You are required to use industry-accepted configuration and hardening standards when setting up systems that are part of your PCI scope.

Configuration and hardening requirements apply to all computer systems, network devices, and applications used to process or secure cardholder data. This may include things like web servers, database software, firewalls, point-of-sale systems, or workstations used to process credit card transactions.

Examples of system hardening practices include:

- Disabling services and features you don't use
- Uninstalling applications you don't need
- Limiting servers to perform a single role
- Removing or disabling default accounts

- Changing default passwords
- Configuring other security settings

Permitting anything unnecessary to remain on a system could introduce vulnerabilities and open you up to additional risk.

Often, organizations get overwhelmed trying to understand how and where to begin implementing system configuration standards, especially in an environment that has expanded and changed over time.

The first step in securing your environment to meet PCI standards is to understand where credit card data is stored, processed, and transmitted. Begin by documenting the flow of cardholder data through your environment, making a list of each system, device, and application it touches along the way. Next, look at the systems and applications that, while not directly touching the data, can affect the security of those that do. Add this information to your documentation.

The key to effective system configuration and hardening is consistency. Once you have identified the systems and applications that need attention and documented a standard that meets your environment's requirements, make sure processes are in place to follow this standard as time goes on. Keep your standard and process up to date as your business changes and as you discover new threats and vulnerabilities.

Automated tools can simplify the task of enforcing configuration standards, allowing administrators to quickly discover systems that are out of compliance.

REQUIREMENT 2 IT CHECKLIST

Configuration Standards

Assigned to:_____

Assignment date:_____

Things You Will Need To Have:

A secure way to access and manage systems in your environment

An inventory of all hardware and software used in your CDE

Documented configuration standards for all types of systems in your CDE

NOTES

Things You Will Need To Do:

Assign system administrator and knowledgeable personnel the responsibility of configuring system components.

Implement a system hardening guide covering all components of your CDE.

Disable and uninstall any unnecessary programs, services, guest accounts, scripts, drivers, features, subsystems, file systems, and web servers.

Document which services and programs are allowed.

Change vendor-supplied default usernames and passwords. Remove or disable unnecessary default accounts before installing a system on the network (e.g., operating systems, security software, POS terminals, routers, firewalls, SNMP).

Document security policies and operation procedures for managing vendor defaults and other security settings. Inventory all systems within scope of the payment application environment and keep inventory up to date.

Things You May Need To Do:

Use technologies, such as VPN, for web-based management and other non-console administrative access. Ensure all traffic is encrypted according to current standards.

If wireless Internet is enabled in your CDE, change wireless default settings including encryption keys, passwords, and SNMP community strings.

Enable only one primary function per server (e.g., logging server, web server, DNS).

NOTES

Requirement 3

Protect Stored Account Data

ENCRYPT CARDHOLDER DATA

According to requirement 3, stored card data must be encrypted using industry-accepted algorithms (e.g., AES-256). The problem is many organizations unknowingly store unencrypted primary account numbers (PAN), which typically happens because of mis-configured software.

Not only must card data be encrypted, but the encryption keys must also be protected. Not protecting the encryption key location using a solid PCI DSS encryption key management process is like storing your house key in your front door lock.

Assign the responsibility of keeping unencrypted card data off your systems to an individual or team. Have this person or team define, document, and follow a process of periodic data discovery cycles to recheck and ensure systems remain clean of unencrypted card data.

KNOW WHERE ALL CARDHOLDER DATA RESIDES

An essential part of eliminating stored card data is using a valid card data discovery tool and methodology. These tools help identify the location of an unencrypted PAN, so you can securely delete or encrypt it. They also help identify which processes or flows might need to be fixed.

Remember, payment card data can easily leak due to poor processes or misconfigured software. Start by looking where you think the data is, and then look where it shouldn't be.

You should create and document a current cardholder flow diagram for all card data flows in your organization. A cardholder data (CHD) flow diagram is a graphical representation of how card data moves through an organization. As you define your environment, it is important to ask all organizations and departments if they receive cardholder information, and define how their answers may change CHD flows.

2023 PANSCAN® DATA ANALYSIS

Storage of unencrypted payment card data increases an organization's risk and liability in the event of a data breach.

Since 2010, SecurityMetrics PANscan® has discovered over 3 billion unencrypted PANs on business networks. In 2022, users scanned over 2,400 computers and 296.75 TBs.⁹ Here are key statistics:

+3.7 Million

Primary Account Numbers found

5%

stored track data (i.e., data
inside magnetic stripe)

86%

of PANscan® users
discovered unencrypted
PAN data

To accurately craft your CHD flow diagram, ask yourself:

- What device(s) am I using for transactions? A virtual terminal? POS system?
 - What happens to the card data after a transaction?
 - When is data encrypted? Is it even encrypted at all?
- Do I store card data before it's sent to the processor for approval?
 - How does settlement occur? Does settlement occur real time or at the end of the day?
 - How is data authorized and returned by the processor?
- Is card data backed up on my system? Are backups encrypted? Is the backup server at a different data location?
 - Where might card data be going or moved in processes not part of authorization and settlement?

Below is a table which describes which CHD elements can and cannot be stored, as well as when encryption is required:

MILESTONES	GOALS	STORAGE ALLOWED	ENCRYPTION REQUIRED
Cardholder Data	Primary account number (PAN)	Yes	Yes
	Cardholder name	Yes	No
	Service code	Yes	No
	Expiration date	Yes	No
Sensitive Authentication Data	Full track data	No	Not allowed to store
	CAV2/CVC2/CVV2/CID	No	Not allowed to store
	PIN/PIN block	No	Not allowed to store

Requirement 3: Protect Cardholder Data



BEN CHRISTENSEN

SecurityMetrics Senior Security Analyst
CISSP | CISA | QSA

Don't keep any data you don't need. If you only need the last four numbers of PAN, get rid of the rest! For each element of cardholder data, ask yourself if you really need it or if it is just nice to have. I have found that some companies have a lot of data they really don't need and never ask if the business needs it. The more data you keep, the higher the risk.

IT should work closely with all business groups to decide what data the company needs, where to store it, and for how long. Data retention policies are key to ensuring that your data has the appropriate controls. Periodic assessments of data retention and data mappings should be performed. Data requirements might change over time, so check often.

It is important to know what data you actually store, process, and/or transmit. If you don't know what you have, it is difficult to implement the correct controls around it. Data flow mapping helps you understand the data coming into and out of your

**The more data you keep,
the higher the risk.**

organization. Create data flow diagrams for your entire organization (on all information you deem sensitive), not just for your CDE environments. You might miss something if you only focus on the CDE and CHD.

In addition, use automated tools that can help you search for and find unencrypted CHD. You will be surprised by what you find outside of your CDE. Run these tools often to ensure data is where it should be.

PCI DSS v4.0 Considerations for Requirement 3

As noted above in the PCI DSS v4.0 summary, Requirement 3 has a lot of changes. Make sure you understand what elements of cardholder data you are storing and what that means for 4.0. There are some changes to the encryption requirements in 2025. These changes could take a lot of effort, so start now.

Also, review your algorithms and hashing functions as those may be impacted when moving to PCI DSS v4.0.

REQUIREMENT 3 IT CHECKLIST

Securing Cardholder Data

Assigned to:_____

Assignment date:_____

- Things You Will Need To Have:
- A documented data retention policy
 - A data flow diagram
 - A data discovery tool

NOTES

Things You Will Need To Do:

- Have employees acknowledge their training and understanding of the policy
- Eliminate storage of sensitive authentication data after card authorization
- Encrypt sensitive authentication data while it is stored before authorization (PCI DSS 4.0)
- Issuers will need to encrypt sensitive authentication data they are storing (PCI DSS 4.0)
- Prevent the copying and relocation of PAN when connecting remotely (PCI DSS 4.0)
- Mask out PAN on customer receipts
- Understand guidelines for handling and storing cardholder data
- Can no longer use disk level encryption to protect card data (only use for removable media) (PCI DSS 4.0)
- Must use a keyed cryptographic hashing method (PCI DSS 4.0)

Things You May Need To Do:

- If PAN data is stored for business or legal reasons, details must be masked, truncated, or secured by strong cryptography.
- PAN storage should be accessible by as few employees as possible for business or legal reasons. This includes limited access to cryptographic keys, removable media, or hard copy of stored details.

NOTES

Requirement 4

Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

For requirement 4, you need to identify where you send cardholder data. The following are common places primary account numbers (PAN) are sent:

- Processors
- Backup servers
- Third parties that store or handle PAN
- Outsourced management of systems or infrastructure
- Corporate offices

You need to use encryption and have security policies in place when you transmit cardholder data over open, public networks.

STOP USING SSL/EARLY TLS

Based on vulnerabilities in web encryption, discontinue or remove all instances of SSL and early TLS.

Your systems may still be using SSL and early TLS, so you should contact your terminal providers, gateways, service providers, vendors, and acquiring banks to determine if the applications and devices you use have this encryption protocol.

Examples of applications that might still use SSL/early TLS include:

- POS/POI hardware terminals
- Virtual payment terminals
- Back-office servers
- Web/application servers

The PCI Council believes that SSL and early TLS will no longer protect cardholder data.

Please note that organizations using POS/POI terminals with existing implementations of SSL and early TLS must ensure that the devices in use are not susceptible to any known exploits for these insecure protocols. Check with your merchant bank or POS/POI supplier if you have questions about that.

Requirement 4: Sending Data Over Open And Public Networks



BEN CHRISTENSEN

SecurityMetrics Senior Security Analyst
CISSP | CISA | QSA

Build off of the data flow diagrams discussed in the tips in Requirement 3.³ Know exactly where CHD is coming from and being sent to, inside and outside of your organization. Make sure your CHD is encrypted when transmitted over open public networks using strong and industry accepted encryption technologies.

Are you using strong encryption on all CDE impacting services? I have noticed that some companies are still using older technologies even though the latest is also supported. For example, CDE web servers using TLS 1.3 or TLS 1.2 are still accepting connections using TLS 1.1. Disable all insecure protocols and encryption.

Leverage tools that can analyze web services and report any insecure setups.

Companies should also leverage tools that can analyze web services and report any insecure setups. You may not be aware of all your services accessible over the internet. Run these tools often to help ensure you are using acceptable protocols and encryption strengths.

PCI DSS v4.0 Considerations for Requirement 4

Some organizations may have a large number of TLS certificates. Start inventorying those now and remove those certs not needed. 2025 seems far off, but it will come quickly. Don't wait.

REQUIREMENT 4 IT CHECKLIST

Transmitting Cardholder Data

Assigned to:_____

Assignment date:_____

Things You Will Need To Have:

An in-house policy to ensure you do not send unprotected PANs via end-user messaging technologies

NOTES

Things You Will Need To Do:

Check all related device configuration for proper encryption. Check with vendors to make sure supplied POS/POI devices are encrypting data appropriately

Validate that POS/POI devices are not susceptible to any known exploits. Devices and software used to process credit cards need to be PCI DSS compliant

Review all locations where CHD is transmitted or received. Examine system configurations. Review all devices and systems to ensure you use appropriate encryption within your CDE. You must safeguard sensitive cardholder data during transmission over open, public networks

Use only trusted keys and certificates. Check inbound/outbound transmissions and verify that encryption keys and certificates are valid. Use secure configurations and proper encryption strengths. Do not support insecure versions or configurations. This means you will continually need to check for the latest encryption vulnerabilities and update as needed

Review and implement documented encryption standard best practices

Review and implement policies and procedures for sending and receiving credit card data

Examine system configuration and adjust encryption configuration as needed

Document, track, and inventory SSL and TLS certificates in use for the transmission of sensitive data across public networks (PCI DSS 4.0)

Things You May Need To Do:

Make sure TLS is enabled whenever cardholder data is transmitted or received through web-based services.

Check wireless network encryption standards

Examine keys and certificates

Prohibit the use of WEP—an insecure wireless encryption standard

NOTES

Requirement 5

Protect All Systems and Networks
from Malicious Software

REGULARLY UPDATE YOUR ANTI-MALWARE

Anti-malware software needs to be installed on all systems commonly affected by malware, regardless of its location. Make sure anti-malware or anti-virus programs are updated on a regular basis to detect known malware. Maintaining an up-to-date anti-malware program will prevent known malware from infecting systems.

Depending on your relationship with your POS vendor, they may or may not maintain your anti-malware scanning. If your vendor doesn't handle your anti-malware, it's up to you to ensure regular scanning is conducted.

Using outside sources such as the United States Computer Emergency Readiness Team (US-CERT), SANS Institute, and vendor/anti-malware threat feeds, you can identify emerging malware and attacks on systems. Then configure systems to alert and report suspicious activity, such as new files added to known malware directories or unauthorized access attempts.

Vigilant vulnerability management is the most effective way for you to proactively reduce the window of compromise, greatly narrowing the opportunity for malicious actors to successfully attack your systems and steal valuable data. As part of your vulnerability management strategy, make sure to include updated anti-malware software.

**Anti-malware
software needs
to be installed on
all systems
commonly affected
by malware,
regardless of
its location.**

Requirement 5: Implement And Update Your Anti-Malware



MICHAEL OHRAN

CISSP | CISA | QSA | SSF | SSL

System administrators have the responsibility of making sure their anti-malware software, including the signatures, are up to date.

After a software upgrade, verify that signatures are able to be updated. The new software may use different firewall rules or directory permissions, requiring some system configuration changes to ensure signature updates continue.

PCI DSS requires anti-malware software to be installed on all systems that are commonly affected by malware (e.g., Windows). While Linux servers are often considered systems not commonly affected by malware, it's highly recommended that anti-malware software be installed for any Internet-facing Linux servers.

System administrators are responsible for making sure that their anti-malware software are up to date.

PCI DSS v4.0 Considerations for Requirement 5

In PCI DSS v.4.0, Requirement 5 is broadened by using the term *anti-malware* instead of *anti-virus*. Most solutions have already expanded past simply protecting against “viruses,” but it might be time for a more comprehensive solution.

Several new requirements were added. Though not enforced until April 2025, start implementing them sooner. Finding the appropriate solution to help against phishing attacks will be interesting, and will not necessarily be inside the CDE.

REQUIREMENT 5 IT CHECKLIST

Anti-Malware Updates

Assigned to:_____

Assignment date:_____

- Things You Will Need To Do:
- Deploy anti-malware program on commonly affected systems

Protect all systems against malware and regularly update anti-malware software or programs

Set anti-malware to detect and remove all known types of malicious software

Maintain and evaluate audit logs with IT staff

Set anti-malware program to scan automatically

Make sure anti-malware program is updated automatically (with signatures kept current)

Ensure anti-malware program cannot be disabled or altered by users (i.e., admin access only)

Document and review malware procedures; review with necessary staff

Examine system configurations and periodically evaluate malware threats to system

NOTES

Requirement 6

Develop and Maintain Secure Systems and Software

REGULARLY UPDATE AND PATCH SYSTEMS

Application developers will never be perfect, which is why updates to patch security holes are frequently released. Once a threat actor knows they can get through a security hole, they pass that knowledge to other criminals who could then exploit this weakness until a patch has been deployed.

Quickly implementing security updates is crucial to your security posture. Patch all critical components in the card flow pathway, including:

- Internet browsers
- Firewalls
- Application software
- Databases
- POS terminals
- Operating systems

Older Windows systems can make it difficult for merchants to remain secure, especially when the manufacturer no longer supports a particular operating system or version (e.g., Windows 7, Windows Server 2008 R2).

Operating system updates often contain essential security enhancements that are specifically intended to correct recently exposed vulnerabilities. When using an unsupported OS that doesn't receive such updates and patches, the vulnerability potential increases exponentially.

Be vigilant about consistently updating software associated with your system. Requirement 6 details that organizations must "install critical patches within a month of release" to maintain compliance.³ Don't forget about critical software installations like credit card payment applications and mobile devices. To stay up to date, ask your software vendors to put you on their patch and upgrade notification list.

Keep in mind that the more systems, computers, and apps your company has, the more vulnerabilities it may be exposed to.

Another way to stay on top of vulnerabilities is through vulnerability scanning, which is arguably the easiest way to discover software patch holes that cyber criminals would use to exploit, gain access to, and compromise an organization.

ESTABLISH SOFTWARE DEVELOPMENT PROCESSES

If you develop payment applications in house (e.g., ecommerce websites, POS applications), you must use strict development processes and secure coding guidelines as outlined in the PCI DSS. Don't forget to develop and test applications according to industry accepted standards like the Open Web Application Security Project (OWASP).

Be vigilant about consistently updating the software associated with your system.

WEB APPLICATION FIREWALLS

Requirement 6 requires public-facing web applications to regularly monitor, detect, and prevent web-based attacks, such as implementing web application firewalls (WAF) in front of public-facing web applications. Even though these solutions can't perform the many functions of an all-purpose network firewall (e.g., network segmentation), they specialize in one specific area: monitoring and blocking web-based traffic.

A WAF can protect web applications that are visible or accessible from the Internet. Your web application firewall must be up to date, generate audit logs, and either block cyber-attacks or generate a security alert if it detects attack patterns.

WEB APPLICATION FIREWALL PROS

- Immediate response to web application security flaws
- Protection for third-party modules used in web applications
- Deployed as reverse proxies

WEB APPLICATION FIREWALL CONS

- Requires more effort to set up
- Possibly break critical business functions (if not careful)
- May require some network re-configuration

Requirement 6: System Updating And Software Development



MICHAEL OHRAN

CISSP | CISA | QSA | SSF | SSL

System administrators have the responsibility to ensure that all system components (e.g., servers, firewalls, routers, workstations) and software are updated with critical security patches within 30 days of public release. If not, these components and software are vulnerable to malware and security exploits.

Quickly implementing security updates is crucial to your security posture.

Systems or software might be excluded from updates because they weren't able to communicate with the update server (e.g., WSUS, Puppet). This broken communication could have resulted from a network or system configuration change. It's imperative that system administrators are alerted when security updates fail.

Another important subsection of requirement 6 is the need to have proper change control processes and procedures. Change control processes should include at least the following:

- Development/test environments must be separate from production with proper access control in place to enforce access rights.
- Separation of duties must be implemented between personnel assigned to development/test environments and those assigned to production.
- Production data (e.g., live credit card numbers, live personally identifiable information) must never be used in test/development environments.
- All test data and accounts must be removed before a production system becomes active.
- Change control procedures related to implementing security patches and software modifications must be documented.

Companies need to embrace the idea of change control for their software development and system patching/updating.

Companies need to embrace the idea of change control for their software development and system patching/updating. There are four requirements detailed by the PCI Council of what a proper change control procedure must contain:

1. Changes must have a documented explanation of what will be impacted by the change.
2. Changes must have documented approval by authorized parties.
3. Changes to an organization's production environment must undergo proper iterations of testing and QA before being released into production.
4. Change control procedures must always include a back-out or roll-back procedure in case the updates go awry.

When developing software (e.g., web applications), it's crucial that organizations adopt industry-accepted standards or best practices for coding, such as OWASP. This will guide them in enforcing secure

coding practices in their application development process and keep software code safe from malicious vulnerabilities (e.g., cross-site scripting, SQL injection, insecure communications, CSRF).

Insecure communications, for example, have been in the spotlight since SSL and TLS 1.0 are no longer considered acceptable protocols when data is being transmitted over open, public networks. Everyone should be on TLS 1.2+ now.

PCI DSS v4.0 Considerations for Requirement 6

Requirements have been moved around and grouped together where they are related.

New requirements have been added, notably that all scripts loaded onto the payment page of the consumer's browser must be managed. New solutions and services are being developed to assist with

Also, a web application firewall is no longer optional.

REQUIREMENT 6 IT CHECKLIST

Software Updates

Assigned to:_____

Assignment date:_____

- Things You Will Need To Have:

 - Vendor supported programs, operating systems, and devices
 - Access to an update server (i.e., repository for systems to get updates)
 - A change management process
- Things You Will Need To Do:

 - Have a process in place to keep up to date with the latest identified security vulnerabilities and their threat level
 - Install all vendor-supplied security patches on all system components
 - Ensure all security updates are installed within one month of release
- Things You May Need To Do:

 - Set up a manual or automatic schedule to install the latest security patches for all system components

NOTES

Requirement 7

**Restrict Access to System
Components and Cardholder
Data by Business Need to Know**

RESTRICT ACCESS TO CARDHOLDER DATA AND SYSTEMS

You should have a role-based access control (RBAC) system, which grants access to cardholder data and systems on a need-to-know basis. Configuring administrator and user accounts helps prevent exposing sensitive data to those who don't need to know this information.

PCI DSS requires a defined and up-to-date list of the roles with access to the cardholder data environment.³ On this list, you should include each role, the definition of each role, access to data resources, current privilege level, and what privilege level is necessary for each person to perform their normal business responsibilities. Users must fit into one of the roles you outline.

Have a defined and up-to-date list of roles with access to the card data environment.

User access isn't limited to your normal office staff. It applies to anyone needing access to your systems behind the desk, such as an IT group or maintenance professional. You need to define and document what kind of user permissions they have.

**Never Have
a False Sense
of Security.™**

**Learn More About
SecurityMetrics
PCI DSS Audits.**

[Learn More](#)

Requirement 7: Restrict Access



MICHAEL OHRAN

CISSP | CISA | QSA | SSF | SSL

This requirement is one of the oldest and most basic parts of the PCI DSS (and data security in general).

There's no new trend or solution. But not all organizations accurately comply with this requirement or have even tried role-based access at all.

This is all you need to know: don't give access to people who don't need it. Cardholder data and card systems should only be accessible to those that need that information to do their jobs. Once you've implemented access privileges, make sure to document it.

Cardholder data and card systems should only be accessible to those that need that information to do their jobs.

PCI DSS v4.0 Considerations for Requirement 7

PCI DSS 4.0 raises the expectations of managing user accounts, system accounts, and access privileges. More frequent reviews are required. Prepare for the new requirements by thoroughly documenting all accounts and related access privileges.

REQUIREMENT 7 IT CHECKLIST

Establish Access Control

Assigned to:_____

Assignment date:_____

Things You Will Need To Have:

Written policy detailing access controls for systems in the CDE

Required Features:

Document access control policies based on job classification and function

Roles and privilege levels defined

“Deny all” rule in place for access control systems

Things You Will Need To Do:

Detail a written policy to include access to cardholder data based on job roles with privilege level, and approval/documentation of employee access

Document policies in place with each employees’ role/ access and train employees on their specific access level

Things You May Need To Do:

Implement access controls on any systems where cardholder data is stored and handled

Configure access controls to only allow authorized parties and deny all others without prior approval or access

NOTES

Requirement 8

Identify Users and Authenticate Access to System Components

WEAK PASSWORDS AND USERNAMES

If a username or password doesn't meet the recommended security standards for length, uniqueness, and complexity, you will be a soft target for an attacker that is trying to gain access to your environment and sensitive information. One approach that an attacker may take is to try a brute-force attack against a system by guessing the password of a user account. Once the attacker has gained access, they will then work to escalate their account privileges and move laterally through a variety of attack vectors.

Having a nondescript username and a strong password will make guessing your login credentials exponentially more difficult and keep your authentication method from being a soft target. Additionally, work with development to ensure the error responses are the same latency regardless whether the username is valid or not.

PCI DSS requirement 8 specifies that passwords must be changed every 90 days (the new password cannot be the same as any of the previous four passwords used) and must be comprised of at least seven characters of both numbers and letters. Beginning on March 31, 2025, passwords will need to be at least 12 characters long.

Passwords that fall short of this criteria can easily be broken using a password-cracking tool, rainbow table or through social engineering. As computing power increases, what seems like a good password may in reality be easy to break.

The longer the password or passphrase and the more character formats and words from other languages included, it will be exponentially more difficult for an attacker to crack that password.

With this security comes a risk posed by human nature. When a password is too hard to remember, it is often written down and placed in an easy to access location. Be sure to review and update your company password policy so that increasing the complexity doesn't undermine security objectives. Some companies use a password wallet that the company controls in order to ensure compliance with periodic password changes, length, and complexity policies for their employees.

ACCOUNT MANAGEMENT

PCI requires the disabling of default accounts and having unique user and admin account names instead of using system defaults or common usernames (i.e., admin, an organization's name, or a combination of the two). A company is much more secure if an attacker has to first guess the username before cracking its corresponding password.

Be sure that an account lock-out is set to at most six consecutive failed login attempts within a 30-minute period. Requiring an administrator to manually unlock accounts will discourage automated hacking methods.

The more manual steps malicious actors have to go through, the more likely it is they will move on to an easier target.

IMPLEMENT MULTI-FACTOR AUTHENTICATION

System security should not be based solely on the complexity of a username and password, and no password should be considered uncrackable. That's why multi-factor authentication (MFA) is an effective solution to secure remote access and is a requirement under the PCI DSS.¹⁰

Configuring multi-factor authentication requires at least two of three following factors:

- Something you *know* (e.g., a username and password, PIN number)
- Something you *have* (e.g., hardware token, smartcard)
- Something you *are* (e.g., a fingerprint, ocular scan, voiceprint)

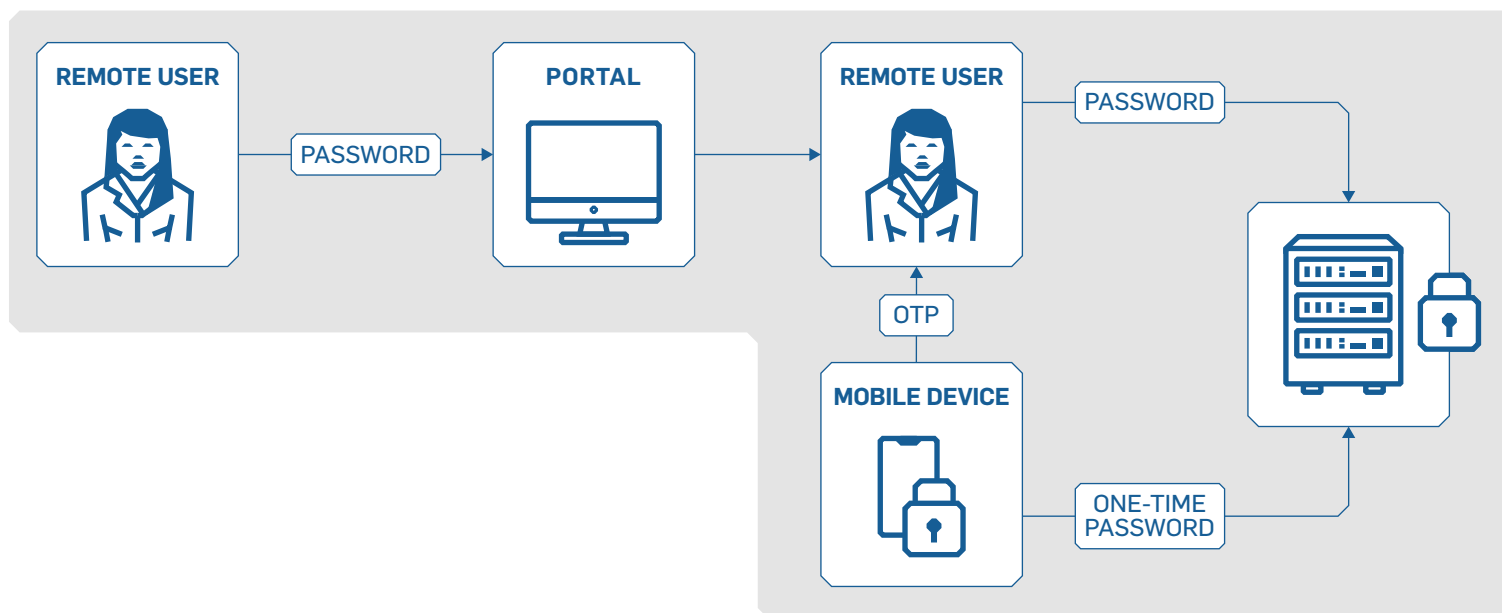
Your authentication mechanisms should be out-of-band and independent of each other. There should be a physical separation between mechanisms, so that access to one factor does not grant access to another, and if one factor is compromised, it does not affect the integrity and confidentiality of any other factor.

Additionally, make sure that you “incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.”³

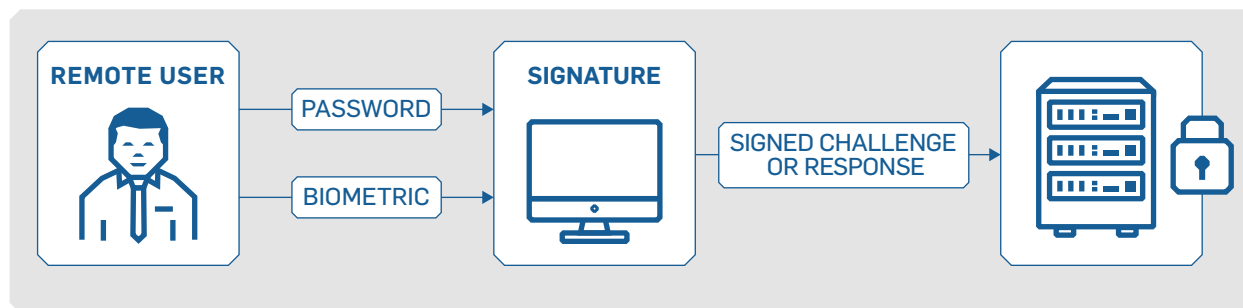


A few examples of effective multi-factor authentication for remote access could include:

Example 1: The remote user enters their username and password, and then must enter an authentication code that is available to them through an RSA token in their possession.



Example 2: The remote user enters a password and biometric to log in to a smartphone or laptop. The individual then provides a single authentication factor (e.g., another password, digital certificate, signed challenge response) to connect to the corporate network.



If a remote access application configuration only requires a username and password to access sensitive data or systems and devices that store, process, or transmit cardholder data, the application has been configured insecurely.

Requirement 8: Use Unique ID Credentials



MICHAEL MAUGHAN

SecurityMetrics Security Analyst
CISSP | CISA | QSA

Requirement 8 is all about having unique ID information. For example, you must have your own unique ID credentials and account on your systems and devices so that you can prove with audit log files who committed the error or malicious action. With a shared account a malicious user could simply blame the other users that use the same account.

As a system administrator, best practice is to have a regular account that is used for day-to-day work on your portable device and a different administrative account when performing administrative functions on the systems you manage.

Security professionals recognize that passwords are no longer sufficient to secure data. While passwords are still required, they simply are not secure enough. You must set strong, long passwords. If you use a passphrase be sure to include words from various foreign languages, this will make a brute force attacker have to use multiple dictionaries rather than just one, which increases the time to crack the passphrase substantially.

An easy way to remember complex and long passwords is by using passphrases. Passphrases are groups of words with spaces in between (e.g., "Boba Fett in 1983 ROJ was WAY better than 2022 BoBF!"). A passphrase can contain symbols and upper- and lower-case letters. It doesn't have to make sense grammatically. Passphrases are generally easier to remember but more difficult to crack than shorter passwords.

In addition to strong passphrases, password manager software can help you use different passwords for all of your accounts.

You need different passwords for different services so that if one service gets compromised the attacker is unable to access other services with those credentials.

If your email account password is compromised and you use the same password across several devices, or even use that email address to receive the reset password emails from several websites, you have a major security problem on your hands.

Something to be aware of with brute force attacks is the latency difference between an error that has a valid username and one that does not. If the response has more or less latency than a normal username error response, then the attacker will know that username is likely a valid username. Next the attacker will try to brute force the password of that newly discovered user account. So it's good practice to make all authentication errors respond with the same latency.

Another practice to consider is having a company managed password wallet that the company controls in order to ensure compliance with periodic password changes, length, and complexity policies for their employees.

REQUIREMENT 8 IT CHECKLIST

Establish Access Control

Assigned to:_____

Assignment date:_____

Things You Will Need To Have:

- Multi-factor authentication for all remote access
- Account management policies and procedures
- Documented approval for changes to account access
- Database access restrictions

Required Features:

- Document access control policies based on job classification and function
- Roles and privilege levels defined
- “Deny all” rule in place for access control systems

Do not use generic accounts, shared group passwords, or generic passwords.

NOTES

Things You Will Need To Do:

Monitor all remote access accounts used by vendors, business partners, or IT support personnel when the account is in use.

Disable all remote access accounts when not in use.

Enable accounts used for remote access only when they are needed.

Implement a multi-factor authentication solution for all remote access sessions.

Configure multi-factor authentication with at least two of the following methods:

- Something you *know* (e.g., password and username)

- Something you *have* (e.g., one-time password)

- Something you *are* (e.g., fingerprint or retinal scan)

NOTES

Requirement 9

Restrict Physical Access to Cardholder Data

CONTROL PHYSICAL ACCESS TO YOUR WORKPLACE

Employees may think physical security only applies after hours. However, most data thefts (e.g., social engineering attacks) occur in the middle of the day.

Mitigate the risk of physical threats by implementing physical security policies and procedures that preserve onsite business security for your critical assets and data. For example, if you keep confidential information, products, or equipment in the workplace, secure these items in a locked area. If possible, limit outsider access to one monitored entrance, and (if applicable) require non-employees to wear visitor badges.

Don't store sensitive information in the open. Many companies that have services requiring repeat billing or batch processing keep physical copies of credit card information in easily accessible areas for convenience. While this collection of paper copies may make life easier, it puts valuable cardholder data at risk of theft unless appropriate controls are in place.

Employee access to sensitive areas should be controlled and must be related to an individual's job function.

To comply with this PCI DSS requirement, you must document:

- Who has access to secure environments and why they need this access
- What, when, where, and why devices are used
- A list of authorized device users
- Locations where the device is and is not allowed
- What applications can be accessed on the device
- Logging of access attempts

Access policy and procedure documentation must be kept up to date and followed, especially when individuals are terminated or their job roles and responsibilities change.

Best practice is not to allow these removable devices to leave the office, but if they do, consider attaching external GPS tracking and remote wipe technology on all laptops, tablets, external hard drives, flash drives, and mobile devices.

The majority of physical data theft takes only minutes to plan and execute.

Make sure all workstations and mobile devices have an automated timeout or logout (e.g., a password-protected screensaver pops up on a computer after a set amount of time). This reduces the window of opportunity for unauthorized users to access data from these devices and systems when nobody is looking.

KEEP TRACK OF POS TERMINALS

Organizations that use POS systems, PIN pads, and mobile devices or kiosks are required to do three new things:

1. **Maintain an up-to-date list of all devices** including physical location, serial numbers, make, and model.
2. **Periodically inspect devices.** You should ensure device surfaces haven't been tampered with, make sure serial numbers match, and check that seals haven't been broken. This could be a very large task depending on the size of your organization. Whether you inspect devices every day or every month is based on your tampering risk level (e.g., publicly accessible 24/7 gas station terminals vs. a behind-the-counter card swipe device). Document your findings.
3. **Provide staff awareness training** for staff who interact with card-present devices on a day-to-day basis (e.g., cashiers), and record the who, what, and when for future reference. Training should include how to report suspicious behavior and what to do when third parties claim they need to work on your system. For example, rather than assuming IT support staff came in last night to install a new device on the side of a terminal, employees should be trained to question if it's supposed to be there, and then to notify management (according to documented incident response policies and procedures).

PHYSICAL SECURITY BEST PRACTICES

Most physical security risks can be prevented with little effort. Here are a few suggestions to improve your physical security:

- While working on your risk assessment, look for physical security risks.
- Lock all office doors and applicable equipment (e.g., mobile devices) when not in use day and night.
- Require passwords to access computers and mobile devices.
- Encrypt your data or don't store data on these devices.
- Use timeout screensavers and privacy monitors on computers.
- Install and use blinds in all office windows.
- Keep logs of who enters and leaves.
- Keep track of devices that go in and out.
- Have policies in place for stolen equipment (e.g., a good incident response plan).
- Train staff against social engineering.
- Limit access to CHD through role-based access.
- Have staff report suspicious activity and devices.
- Monitor sensitive areas with video cameras and store the video logs for appropriate durations.

TRAIN EMPLOYEES EARLY AND OFTEN

While you may understand how to protect customer card information, your employees may not. And as employee turnover is so common, regular security training is crucial to secure your business.

Social engineering is a serious threat to both small and large businesses. A social engineer uses social interaction to gain access to private areas, steal information, or perform malicious behavior. Employees fall for social engineering attacks more often than you may think.

For example, if someone walked into your storefront and said they were there to work on your network and needed you to lead them to the server room, would your employees think twice to verify their identity?

Train your employees to question unusual behavior. Establish a communication and response policy in case of suspicious behavior. Train employees to stop and question anyone who does not work for the company, especially if the person tries to enter the back office or network areas.

Requirement 9: Improve Your Physical Security



MICHAEL MAUGHAN

SecurityMetrics Security Analyst
CISSP | CISA | QSA

Having electronic access on doors, using cameras to monitor all entries and exits to secure areas, implementing multiple levels of access based on a business need, and approving visitor/employee access are all standard controls for physical security.

Once you know what systems you need to protect, put controls in place that can log and restrict access to them (e.g., badge readers). A good risk assessment would determine an appropriate amount of money to spend on controls necessary to mitigate the identified risk. Something that companies often overlook is the access given to delivery personnel for a night drop. Do you know if that delivery person locked the doors when they left?

Today, you see more organizations hosting their systems in outsourced data centers. Data centers generally have great physical security because they pay attention to the basics. They use cameras to monitor all entries and exits, have multiple levels of access (e.g., lobby, mantrap, hallways, data floors, and cages) to segment physical areas and limit access only to individuals who have been authorized. They also use different levels of authentication requiring both badge and biometrics (e.g., fingerprint, retina) for access.

Digital IP-based cameras are becoming more common, making it easier and more cost effective to deploy and monitor camera systems. These cameras can take snapshots of people and then send those snapshots to security supervisors for verification.

Once you know what systems you need to protect, put controls in place that can log and restrict access to them.

It's also necessary to protect card-swipe devices. Merchants must monitor these devices for tampering or complete replacement. Make sure attackers don't substitute, bypass, or steal your terminal. You and your employees must know what the tamper properties are (e.g., seals, appearance, weight) and test them often. Security best practice is to mount devices with tamper-resistant stands, screws and tape. If you are using a validated P2PE solution, make sure to follow the physical security requirements located in the corresponding [P2PE Instruction Manual](#).¹¹

Lastly, it's important to have good security training for your management and employees. Help them understand malicious conduct and motivate them to report suspicious behavior and violations of company policy and procedures.

REQUIREMENT 9 IT CHECKLIST

Improving Physical Security

Assigned to:_____

Assignment date:_____

Things You Will Need To Have:

Policies and procedures that limit the access to your physical media and devices used for processing

NOTES

Things You Will Need To Do:

Restrict access to any publicly accessible network jack.

Keep physical media secure and maintain strict control over any media being moved within the facility and outside of it.

Keep electronic media in a secure area with limited access (e.g., a locked office clearly marked "Management Only") and require management approval before the media is moved from its secure location.

Use a secure courier when sending media through the mail so the location of the media can be tracked.

Destroy media in a way that it cannot be reconstructed; if the media is separated prior to destruction, keep the media in a locked container with a clear label of "To Be Shredded" or something similar.

Maintain a list of all devices used for processing, and train all employees to inspect devices for evidence of tampering. Training should include a process for verifying the identity of outside vendors wanting access to the machine, a process for reporting suspicious behavior around the machine, and a system to ensure employees know not to replace devices without management approval.

Things You May Need To Do:

A set process to train employees about proper device management and a way to report any suspicious behavior around the processing device.

A secure location to keep media, including a second secure location, if business practice is to separate media no longer needed.

A good risk assessment of the threats and vulnerabilities related to physical security.

NOTES

Requirement 10

Log and Monitor All Access to System Components and Cardholder Data

SYSTEM LOGS AND ALERTING

System event logs are recorded pieces of information regarding the actions taken on computer systems like firewalls, office computers, or payment applications.

Log monitoring systems (e.g., Security Information and Event Management [SIEM] tools) oversee network activity, inspect system events, alert you to suspicious activity, and store user actions that occur inside your systems. Think of these systems as a lookout, providing you with data breach alerts. The raw log files are also known as audit records, audit trails, or event logs.

Most systems and software generate logs including operating systems, Internet browsers, POS systems, workstations, anti-malware, firewalls, and IDS/IPS. Some systems with logging capabilities do not automatically enable logging, so it's important to ensure all systems create and collect logs. Some systems generate logs but don't provide event log management solutions. Be aware of your system capabilities and install third-party log monitoring and management software as needed.

ESTABLISHING LOG MANAGEMENT

Logs should be collected and sent to a central location, whether an onsite logging server or an online service. Businesses should review their logs daily to search for errors, anomalies, or suspicious activities that deviate from the norm.

From a security perspective, the purpose of a log alert is to act as a red flag when something potentially malicious is happening. Reviewing logs regularly helps identify issues in your system. Given the large amount of log data generated by systems and networking devices, it's impractical to manually review all logs each day; plus, PCI DSS v4.0 requires automated mechanisms to perform audit log reviews.

Log monitoring software takes care of this issue by using rules to automate log review and only alert on events that might be real issues. Often this is done using real-time reporting software that alerts you via email or text when suspicious actions are detected.

Often, log monitoring software comes with default alerting templates to optimize monitoring and alerting functions immediately. However, not everyone's network and system designs are the same, and it's critical to correctly configure what is being monitored and the alerting threshold rules during setup.

Logs are only useful if they are regularly reviewed.

LOG MANAGEMENT SYSTEM RULES

Here are some event actions to consider when setting up your log management system rules:

- Password changes
- Unauthorized logins
- Login failures
- New login events
- Malware detection
- Malware attacks seen by IDS
- Denial of service attacks
- Errors on network devices
- File name changes
- File integrity changes
- System object errors
- Data exported
- Shared access events
- Disconnected events
- File auditing
- New service installation
- New user accounts
- New processes started or running processes stopped
- Modified registry values
- Scans on your firewall's open and closed ports

Organizations should review their logs daily to search for errors, anomalies, or suspicious activities that deviate from the norm.

To take advantage of log management, look at your security strategy and risk assessment and make sure the following steps are taken care of:

- Decide how and when to generate logs.
- Secure your stored logs so they aren't maliciously altered by cybercriminals or accidentally altered by well-intentioned employees.
- Assign responsible personnel the duty to review logs daily.
- Set up a team to review suspicious alerts and determine if they are incidents or false positives.
- Spend time to create rules for alert generation (don't just rely on a template).
- Store logs for at least one year, with three months readily available.
- Frequently check log collection to identify necessary adjustments.
- Identify assets, risks, threats, and vulnerabilities and make sure that all are monitored and settings are configured to generate alerts.
- Confirm everything is being appropriately logged by testing the alert and monitoring configurations

Diligent log monitoring means that you'll have a quicker response time to security events and better security program effectiveness. Not only will log analysis and daily monitoring demonstrate your willingness to comply with PCI DSS requirements, but it will also help defend against internal and external threats.

Requirement 10: Audit Logs and Log Monitoring



MICHAEL MAUGHAN

SecurityMetrics Security Analyst
CISSP | CISA | QSA

It's critical that you configure the log monitoring solution correctly so that the appropriate directories, files, security controls, and events are being monitored. Given the large amount of log data generated by systems, it can be time intensive to manually analyze logs (and automated mechanisms to perform audit log reviews will need to be implemented for PCI DSS v4.0).

You likely need SIEM tools to sift through logs and drill down into problems. In the past, SIEM systems were mainly utilized by large corporations, but solutions for smaller companies are now available.

Organizations often struggle with good log review processes. Using SIEM tools can enable you to have real-time alerting to help you recognize a current attack and initiate your incident response plan.

Regular log monitoring means a quicker response time to security events and improved security program effectiveness.

It is a good idea to test your alerting capabilities as part of your incident response test to ensure alerts are being generated and critical systems and applications are being appropriately monitored.

To correlate events over multiple systems you must synchronize system times. All systems should get their system time from internal time servers, which in turn receive time from a trusted external source.

PCI DSS requires service providers to implement a process to detect and respond to failures of critical security controls in a timely manner. You need to be able to detect these failures and have defined incident responses in place. Your response plans not only need to address the response to fix the problem, but they should also identify risks created by the failure, find root causes, document lessons learned, and implement any necessary changes to prevent failures from happening again.

REQUIREMENT 10 IT CHECKLIST

Improving Physical Security

Assigned to:_____

Assignment date:_____

Things You Will Need To Have:

An automated audit log tracking all security-related events for all system components

Audit logs that track:

Any action taken by an individual with administrative privileges

Failed login attempts

Changes to accounts—including elevation of privileges, account additions, and account deletions

Identification of user, what the event type was, date and time of the event, whether the event was a success or failure, where the event originated from, and the name of affected data, system component, or resource

Things You Will Need To Do:

Have a process in place to review logs and security events at least daily, in addition to any system component reviews, as defined by your organization for risk management strategy or other policies.

Have a process in place to respond to anomalies and exceptions.

Keep all audit log records for at least one year and keep the last three months’ logs readily available for analysis.

NOTES

Requirement 11

Test Security of Systems and Networks Regularly

UNDERSTAND YOUR ENVIRONMENT

The types of systems that make up a business's IT environment influence the kinds of attacks to which they're susceptible; therefore, a security testing plan should be tailored to the environment.

Defects in web browsers, email clients, POS software, operating systems, and server interfaces can allow attackers to gain access to a system. Installing security updates and patches for systems in the cardholder or sensitive data environments can help correct defects and vulnerabilities before attackers have the opportunity to exploit them. A vulnerability scanning process helps to identify vulnerabilities, so they can be corrected.

In the case of custom in-house applications, internal code review and testing, and independent penetration testing, can expose many of the weaknesses commonly found in application code.

These types of scans and tests are the best line of defense in identifying weaknesses, so they can be corrected before deployment.

CHANGE AND TAMPER DETECTION FOR PAYMENT PAGES

One of the biggest v4.0 changes was the addition of requirement 11.6.1, which details that merchants and service providers need to implement a change and tamper detection mechanism for any payment pages. This requirement addition is a direct result of the increase in ecommerce skimming compromises seen on payment pages in recent years.

Specifically, requirement 11.6.1 details exactly how organizations need to implement change detection procedures and technologies to alert personnel to unauthorized modifications to the HTTP headers and contents of the page(s) used to house the TPSP iframe. Such tamper-detection mechanisms must run at least weekly to look for unauthorized modifications to these critical web pages.

This requirement has been included for the following SAQs: SAQ A, SAQ A-EP, SAQ D for Merchant, and SAQ D for Service Providers.

PAYMENT PAGE BASICS

What exactly qualifies as a payment page?

- A web-based user interface containing one or more form elements intended to capture account data from a consumer or submit captured account data. The payment page can be rendered as any one of:
 - A single document or instance,
 - A document or component displayed in an inline frame within a non-payment page,
 - Multiple documents or components each containing one or more form elements contained in multiple inline frames within a nonpayment page.

For example, an SAQ A merchant uses a third-party iframe to perform payment capture, this would qualify as a payment page (and they would need to comply with requirement 11.6.1).

However, if the merchant's website is configured to redirect the customer's browser to the TPSP's payment acceptance page, they would mark this requirement as Not Applicable.

VULNERABILITY SCANNING VS. PENETRATION TESTING

To clarify, vulnerability scanning and penetration testing are two different methods to improve security. Some mistakenly believe vulnerability scans are the same as a professional penetration test.

Here are the two biggest differences:

- A vulnerability scan is automated, while a penetration test includes a live person that runs tests against your network.
- A vulnerability scan only identifies vulnerabilities. During a penetration test, the tester attempts to exploit discovered vulnerabilities to gain access to secure systems or sensitive data.

Vulnerability scans and penetration tests work together to identify weaknesses and encourage overall system security.

Vulnerability scans are an easy way to gain weekly, monthly, or quarterly insight into the status of your systems, while penetration tests are a more thorough way to evaluate overall security.

VULNERABILITY SCANNING BASICS

A vulnerability scan is an automated, high-level test that looks for and reports potential vulnerabilities in systems and applications.

PCI DSS requires two types of vulnerability scanning: internal and external. Think of your environment as a house. External vulnerability scanning is like checking to see if doors and windows are locked, while internal vulnerability scanning is like testing to see if bedroom and bathroom doors have locks that would prevent an intruder from moving to more sensitive areas once they have gained access to the house.

An *external vulnerability* scan is performed from outside of your network and identifies known weaknesses in perimeter network devices, servers, or applications. All external IPs and domains exposed in the CDE, or that can provide access to the CDE, are required to be scanned by a [PCI Approved Scanning Vendor \(ASV\)](#) at least quarterly. A PCI ASV is required to go through a rigorous yearly recertification process, during which each ASV runs their scanning tool against PCI Council-provided sites planted with vulnerabilities to test which ones the tool finds and which ones it misses.

An *internal vulnerability* scan is performed from within your network, and it looks at other hosts on the same network to identify internal vulnerabilities. These scans are also required to be performed at least quarterly for PCI compliance. There are a variety of tools to help you comply with internal vulnerability scan requirements. For example, you can:

- Purchase an internal vulnerability scanning tool from your ASV or another provider.
- Download an open source vulnerability scanning tool.

Keep in mind that the scanning tool you use still needs to be configured by a security expert after you purchase or download it.

Vulnerability scanning is an automated method to identify potentially harmful vulnerabilities, so you can remediate them to improve system security.

Typically, vulnerability scanning tools will generate an extensive report of discovered vulnerabilities with references for further research on these vulnerabilities. Some reports even offer suggestions on how to fix discovered issues, and links to fixes and patches where available.

Remember, when it comes to vulnerability scanning, your organization is responsible for scan configuration, actual scanning, findings review, and vulnerability remediation. For PCI compliance, *passing* quarterly vulnerability scan reports must be provided. This means that if a vulnerability is discovered during a scan that is a high risk, or that causes the scan to fail, you must work to resolve the issue, and then re-scan the affected system to show it was fixed.

VULNERABILITY SCANNING PROS

- Quick, high-level look at potential vulnerabilities
- Very affordable compared to penetration testing
- Automatic (can be automated to run weekly, monthly, quarterly)

VULNERABILITY SCANNING CONS

- False positives
- Businesses must manually research and correct each vulnerability before testing again
- Does not confirm if a vulnerability is exploitable

PENETRATION TESTING BASICS

Penetration testing takes vulnerability detection to the next level. Penetration testers are people that analyze networks and systems, identify potential vulnerabilities, misconfigurations, or coding errors, and try to exploit them. In simple terms, penetration testers attempt to break into your company's network by exploiting weaknesses the same way a hacker would. However, unlike a hacker, the penetration tester documents and communicates their methods and findings so that you can fix vulnerabilities before an actual hacker gets to them.

A penetration test is a thorough, live examination designed to identify and exploit weaknesses in your system.

Depending on how your business is required to validate PCI compliance, PCI DSS Requirement 11 may call for annual internal and external penetration testing.³ Even if not required for PCI compliance, performing regular penetration testing is a security best practice. Any organization can benefit by using a penetration test to measure the security of a system or application, or an entire network environment.

The time it takes to conduct a penetration test varies based on network size, system complexity, and the individual penetration test staff members assigned. A small environment can be completed in a few days, but a large environment can take multiple weeks.

Typically, penetration test reports contain a detailed description of testing methodologies, vulnerabilities discovered, attacks used, and suggestions for remediation.

In addition to annual penetration tests, perform a penetration test whenever significant infrastructure changes occur to check if these changes introduced new vulnerabilities.

PENETRATION TESTING PROS

- Rules out false positives
- Live, manual tests mean more accurate and thorough results

PENETRATION TESTING CONS

- Time (1 day to 3 weeks)
- Cost (around \$15,000 to \$30,000)

DIFFERENT TYPES OF PENETRATION TESTING

Network Penetration Test

The objective of a network penetration test is to identify security issues with the design, implementation, and maintenance of servers, workstations, and network services. PCI compliance requires these tests be performed from outside, as well as within, your environment, targeting the cardholder data environment at all access points.

Commonly identified issues include:

- Misconfigured software, firewalls, and operating systems
- Outdated, vulnerable, software and operating systems
- Insecure protocols
- Weak authentication practices
- Overly permissive access controls

Segmentation Check

A type of network penetration testing, the objective of a segmentation check is to confirm that firewalls and other controls are preventing access to the cardholder data environment (CDE) and other sensitive environments as intended. Basically, segmentation checks confirm if network segmentation is set up properly. Remember that the PCI definition of a segmented CDE means no communication is allowed from non-trusted or out-of-scope networks and systems.

If you use network segmentation to isolate your CDE and reduce PCI scope, segmentation checks are an annual requirement. For service providers that use segmentation to limit PCI scope, you're required to conduct penetration tests on segmentation controls every six months.

Commonly identified issues include:

- TCP/UDP access is allowed where it is not expected
- ICMP (ping) access is allowed where it should not be

Application Penetration Test

The objective of an application penetration test is to identify security issues resulting from insecure development practices in the design, coding, and deployment of the software.

Commonly identified issues include:

- Injection vulnerabilities (e.g., SQL injection, remote code execution)
- Cross-site scripting vulnerabilities (XSS)
- Broken authentication (i.e., the log-in panel can be bypassed)
- Broken authorization (i.e., low-level accounts can access high-level functionality)
- Improper error handling (sensitive data, or data useful to hackers, exposed in error messages)
- Vulnerable or outdated plugins, libraries, and other application dependencies

Mobile Penetration Test

The objective of a mobile application penetration test is to identify security issues resulting from insecure development practices in the design, coding, and publishing of the software that supports a mobile application.

Commonly identified issues include:

- Insecure local storage
- Information disclosures
- Injection vulnerabilities (e.g., SQL injection, cross-site scripting (XSS), remote code execution)
- Broken authentication (i.e., the log-in panel can be bypassed)
- Broken authorization (i.e., low-level accounts can access high-level functionality)

Wireless Penetration Test

The objective of a wireless penetration test is to identify misconfigurations of authorized wireless infrastructure and the presence of unauthorized access points.

Commonly identified issues include:

- Insecure wireless encryption standards
- Weak encryption passphrase
- Rogue (unauthorized) and unsecured access points

Social Engineering

Social engineering assessments are used to test the effectiveness of an organization's security awareness training. The tester will use typical business scenarios and normal, everyday interactions with personnel to find those that do not follow established security policies and procedures, or are not security minded. The goal of the tester is that of an attacker: to take advantage of the employee and trick them into doing something they shouldn't.

Commonly identified issues include:

- Employee clicked on malicious emails
- Employee allowed unauthorized individuals into secure areas
- Employee connected a randomly discarded or discovered USB to their workstation
- Employee divulge sensitive or secret information

Requirement 11: Testing Security



DAVID PAGE

SecurityMetrics Senior Security Analyst
CISSP | CISA | QSA

If your organization is required to be PCI compliant, don't procrastinate beginning the penetration test process. Finding and engaging a good penetration testing partner can take more time than you realize.

In performing PCI assessments, it is common to see an organization's penetration testing process, from start to finish, taking as long as everything else involved in the assessment combined. If you wait until your QSA is onsite, or until your SAQ is due, to discuss penetration test scope, methodology, and objectives, you may be unable to meet your PCI compliance deadlines. Start thinking about penetration testing months before your PCI deadlines.

Remember, the required annual penetration test can begin before your PCI assessment, but you can't be validated as PCI compliant before the testing is finished.

Perform a penetration test at least yearly and after major network changes.

PCI DSS v4.0 Considerations for Requirement 11

Like other areas of the PCI DSS, the version 4.0 update includes additions and clarifications that impact an organization's vulnerability discovery, testing, and treatment programs.

New internal vulnerability scanning requirements now call for "authenticated" internal scanning. This allows the scanner to simulate a user with access to systems, to better catch vulnerabilities that exist in applications and other software that require users to log in first.

Organizations are now required to define and document their own penetration testing methodology. By doing this, you will be able to clearly communicate infrastructure details, unique attributes of systems and applications, and testing goals and requirements to the penetration testing partner you engage. This allows for more effective testing and more useful results, all in an effort to better secure your environment.

REQUIREMENT 11 IT CHECKLIST

Security Testing

Assigned to:_____

Assignment date:_____

Things You Will Need To Have:

A process for detecting and identifying authorized and unauthorized wireless devices on a quarterly basis. The method should be able to identify all of the following wireless access points:

WLAN cards inserted into system components

Portable or mobile devices attached to system components that create wireless access points (by USB or other means)

Wireless devices attached to a network port or device

An inventory of authorized wireless access points with listed business justifications

A defined process for performing quarterly internal and external vulnerability scans that addresses discovered vulnerabilities and includes re-scanning to confirm remediation

A defined penetration testing methodology that covers testing the perimeter of the CDE and any critical systems, both internal and external

An intrusion detection or prevention system that examines traffic at the perimeter of the CDE to detect potential malicious behavior and malware activity

A change-detection mechanism covering systems within the CDE that detects unauthorized modifications to critical system files, configuration files, content files, and HTTP headers and contents of payment websites

NOTES

Things You Will Need To Do:

Run quarterly internal vulnerability scans using a qualified internal resource or third party (in either case, organizational independence must exist), address discovered vulnerabilities, and then re-scan systems until high-risk vulnerabilities are resolved.

Run quarterly external vulnerability scans (using an ASV), remediate failing items, and then re-scan until all scans have a passing status.

Run internal and external scans after any significant change to systems or the network.

Perform internal and external penetration testing annually and after significant changes, and be prepared to work with the tester to remediate and re-test any discovered issues.

Configure your intrusion detection/prevention system according to the vendor's recommendations, so that it is kept up to date and will alert you if potential compromises are detected.

Configure your change-detection mechanism to alert personnel to unauthorized modification of monitored files, and configure the tools to perform critical file comparisons at least weekly.

Have a process in place to daily respond to alerts generated by your intrusion detection/prevention and change-detection systems.

NOTES

Things You May Need To Do:

If wireless scanning is used to identify wireless access points, scans must be run at least quarterly.

If automated wireless monitoring is used, configure the system to generate alerts to notify personnel if unauthorized devices are detected.

If your organization is a service provider that uses network segmentation to limit PCI scope, make sure your penetration testing procedures confirm that segmentation is operational and isolates all out-of-scope systems from systems in your CDE every six months.

NOTES

Requirement 12

Support Information Security
with Organizational Policies
and Programs

FORMALLY DOCUMENT BUSINESS PRACTICES

Not only do policies and procedures need to be followed, they also need to be documented. Policies should be written down and easily accessible to all employees.

Documentation helps protect your business from potential liability in the event of a breach. Thorough and accurately documented security policies and procedures help forensic investigators see what security measures your company has in place, and demonstrate your company's proactive and committed approach to security.

If you are a service provider, your executive management is required to implement a PCI DSS Charter.³ This charter must establish responsibility for the protection of cardholder data and grant authority to create and implement a PCI DSS compliance program, including overall accountability for maintaining PCI DSS compliance. It must also define how the person responsible for PCI DSS compliance will communicate with executive management.

Third parties (e.g., partners, vendors, service providers) that have access to your CDE or cardholder data present a risk to the security of your environment. You must have a list of all third-party service providers you use, the PCI requirements these service providers impact or manage on your behalf, a process for performing due diligence prior to engaging a third party, and a way to monitor the PCI compliance of each third party you've engaged.

Documents you'll want to include in your security policy:

- Employee manuals
- Policies and procedures
- Technology usage policies
- Third-party vendor engagement process
- Incident response plans

For PCI compliance, documentation of all security measures and actions should be updated regularly.

ESTABLISH A RISK ASSESSMENT PROCESS

PCI requires all entities to perform an annual risk assessment that identifies critical assets, threats, vulnerabilities, and risks. This exercise helps organizations identify, prioritize, and manage information security risks.

Organizations that take a proactive approach to security will use internal and external resources to identify critical assets, assess vulnerabilities and threats against those assets, and implement a risk management plan to mitigate those threats.

A risk assessment should occur at least annually and after significant changes in your environment or business processes.

The purpose of the risk assessment is to help organizations identify potential security vulnerabilities, threats, and risks to come up with an action plan.

Just because a system is vulnerable doesn't mean it's exploitable or even likely to be exploited. Some vulnerabilities may require so many preconditions that the risk of a successful attack is virtually zero.

Part of a risk assessment is to assign a ranking or score to identified risks. This will help establish priorities and provide direction on what vulnerabilities you should address first. Methodically identifying, ranking, and mitigating risks can decrease the time an attacker can access and negatively affect your systems, and over time closes the door to the attack.

PCI DSS TRAINING BEST PRACTICES

If you think your employees know how to secure cardholder data and what they're required to do to be compliant, you're probably mistaken. In fact, most breaches can be traced back to human error. Although most workers aren't malicious, they are human, and often forget security best practices or don't know exactly what is expected of them.

Unfortunately, malicious actors will take advantage of human error to gain access to sensitive data. For example, when employees leave mobile devices in plain sight and unattended, they provide potential access to passwords, multi-factor authentication tokens, and other valuable information. Malicious actors may access networks because employees set up easy-to-guess passwords. And the list goes on.

Often, people are the weakest link in your overall security scheme.

By informing employees about and holding them accountable for their responsibilities, you can better protect your business and customers.



Employees need to be given specific rules and regular training. A security awareness program that includes regular training (e.g., brief monthly training or communications) will remind them of the importance of security, especially keeping them up to date with current security policies and practices. Here are some tips to help employees protect your sensitive data:

- **Communicate often:** Focus each month on a different aspect of data security, such as passwords, social engineering, or email phishing.
- **Give frequent reminders:** Emphasize data security best practices to your employees through emails, newsletters, meetings, or webinars.
- **Train employees on new policies ASAP:** Newly hired employees should be trained on security and PCI policies as quickly as possible.
- **Make training materials easily available:** Intranet sites are a great way to provide access to training and policy information.
- **Set clear expectations:** Don't present training as a list of "Do Nots." Rather, help employees see that they all have a vested interest in protecting the organization and its business.
- **Create incentives:** Reward your employees for being proactive.
- **Regularly test employees:** Create an environment where employees aren't afraid to report suspicious behavior.

Never Have
a False Sense
of Security.™

Learn More About
SecurityMetrics
PCI DSS Audits.

[Learn More](#)

Requirement 12: PCI Compliance Basics



DAVID PAGE

SecurityMetrics Senior Security Analyst
CISSP | CISA | QSA

The risk assessment is where a lot of organizations struggle with PCI compliance. Many treat it as simply another item on the to-do list. In reality, a risk assessment can be the most important part of your overall security and compliance program, since it helps you identify systems, third parties, business processes, and people that are in scope for PCI compliance. Too many companies approach PCI as simply an “IT issue” and are surprised when they realize PCI compliance touches a lot of other business processes and practices. If you aren’t doing a formal risk assessment now and are intimidated by the process, start small and plan to increase the scope of the review each year.

A risk assessment is a great starting point for establishing a successful security and PCI compliance program.

Another area of difficulty, especially for small organizations, is putting together a comprehensive and relevant security awareness program. Don’t be afraid of what you don’t know! Even if you aren’t a security expert yourself, there is a wealth of security-related information available online, and many resources that make it easy to present a polished training program to your employees. This is one area where the help of an outside security expert or partner can be valuable, since security threats are constantly evolving.

PCI DSS v4.0 Considerations for Requirement 12

The annual risk assessment requirement still calls for the identification of assets, threats, and likelihood of exploitation to occur, but it clarifies that the risk assessment is to be targeted toward each PCI requirement that allows an organization the flexibility to define their own testing frequency or controls.

First you must perform a formal risk assessment to ensure that the control will meet the objective of the requirement and address the risk that the original control mitigated.

For example, if you are a retail merchant, you have a requirement to periodically inspect each point-of-interaction device (PINpad) for signs of tampering. How frequently these inspections should occur can vary based on many factors. How frequently you decide to perform them must be based on a formal targeted risk assessment that documents the factors that resulted in your decision.

Another example that requires performance of a targeted risk assessment is if you implement the new Customized Approach to any PCI requirement. If you take this route, you are able to define your own security controls to meet the requirement. However, first you must perform a formal risk assessment to ensure that the control will meet the objective of the requirement and address the risk that the original control mitigated.

Another addition to this requirement section is to define an annual process to review hardware, software, and cryptographic cipher suites and protocols used in your environment to ensure that the

technologies you rely on are kept current and are still supported by vendor-provided updates and security patches.

All organizations are now required to document and confirm their PCI scope annually to ensure all flows and locations of cardholder data are taken into account, and any changes to scope are understood. Service providers must perform this scoping exercise at least every six months.

Additionally, service providers now need a process to make sure that organizational changes don't have a negative impact on PCI compliance and the performance of PCI responsibilities.

REQUIREMENT 12 IT CHECKLIST

Security Testing

Assigned to:_____

Assignment date:_____

Things You Will Need To Have:

Written security policies and procedures that address all PCI requirements

A security awareness program that provides immediate training to new hires, and annual training to all personnel

Documented usage policies for technologies that could impact the security of your CDE (email, Internet access, laptops, cellular phones, remote access, etc)

A documented process for engaging and monitoring the PCI compliance of each service provider that has an impact on your security

A documented incident response plan

NOTES

Things You Will Need To Do:

Perform a risk assessment annually that, at a minimum, covers the processes and technologies that are involved in handling credit card data, and targets any “periodic” requirements you meet using a Customized Approach

Ensure that each employee completes annual security awareness training, and that you annually review your training program to make sure it is relevant

Screen potential employees that will have access to credit card data or the CDE by performing background checks prior to hire

Annually check the PCI compliance status of your third-party service providers Perform annual testing of your incident response plan. Include training for each person who plays a role in responding to a potential incident

Perform a PCI scoping exercise to identify all flows and locations of cardholder data in your environment, and any system, processes, or people that can impact the security of your cardholder data environment

Perform an annual review of all hardware, software, and encryption technologies you use to make sure none of them are outdated or unsupported

Things You May Need To Do:

If you are assessing PCI compliance as a service provider, you are required to establish a charter that assigns responsibility and grants authority to implement your PCI compliance program, including accountability to executive management.

Service providers must perform quarterly reviews to confirm policies and procedures related to PCI compliance are being followed.

Service providers must also perform a PCI DSS scoping exercise every six months, make sure that organizational changes don't negatively impact PCI compliance, and support their customers' requests for information about their PCI compliance and PCI responsibility.

NOTES



How To Prepare For A Data Breach

SECTION CONTENTS

How To Prepare For A Data Breach _____	115	Test Your Incident Response Plan _____	126
What To Include In An Incident Response Plan _____	119	Data Breach Prevention Tools _____	128
Develop Your Incident Response Plan _____	123		

How To Prepare For A Data Breach

You can't afford to be unprepared for the aftermath of a data breach. It's up to you to control the situation and protect your business.

The following section will help you better understand how to successfully stop payment card information from being stolen, mitigate damage, and restore operations as quickly as possible.

INCIDENT RESPONSE PLAN OVERVIEW

INCIDENT RESPONSE PLAN BASICS

Unfortunately, organizations will experience system attacks, with some of these attacks succeeding. If your organization is breached, you may be liable for the following fines, losses, and costs:¹¹

A well-executed incident response plan can minimize breach impact, reduce fines, decrease negative press, and help you get back to business more quickly. In an ideal world (and if you're following PCI DSS requirements), you should already have an incident response plan in place, and employees should be trained to quickly deal with a data breach.

If there is no plan, employees scramble to figure out what they're supposed to do, and that's when mistakes can occur. For example, if employees wipe a system without first creating images of the compromised systems, then you would be prevented from learning what happened and what you can do to avoid re-infection.

DATA BREACH FINES	
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+
TOTAL POSSIBLE COST:	\$50,000 – \$773,000+

INCIDENT RESPONSE PHASES

An incident response plan should be set up to address a suspected data breach in a series of phases with specific needs to be addressed. The incident response phases are:

- Phase 1: Prepare
- Phase 2: Identify
- Phase 3: Contain
- Phase 4: Eradicate
- Phase 5: Recover
- Phase 6: Review

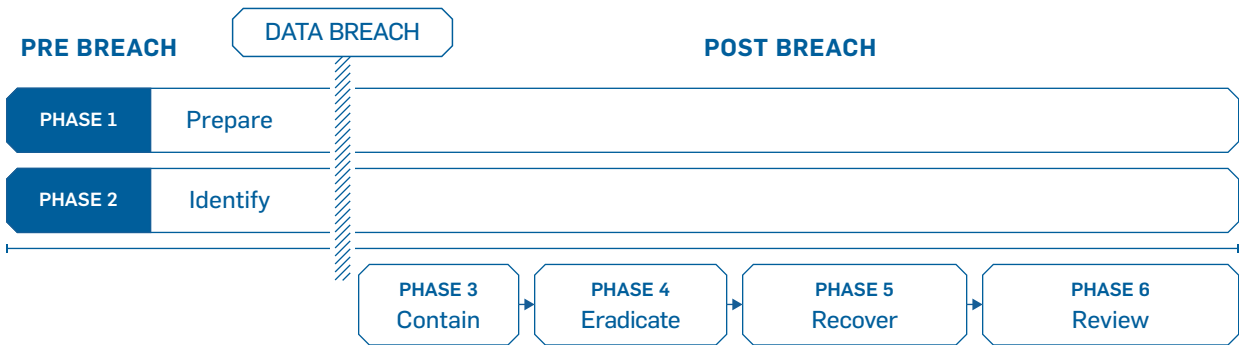
It's important to discover a data breach quickly, identify where it's coming from, and pinpoint what it has affected.

PHASE 1: PREPARE

Preparation often takes the most effort in your incident response planning, but it's by far the most crucial phase to protect your organization. This ongoing phase includes the following steps:

- Ensure your employees receive proper training regarding their incident response roles and responsibilities.
- Develop and conduct tabletop exercises (i.e., incident response drill scenarios) to evaluate your incident response plan.
- Ensure that all aspects of your incident response plan (e.g., training, hardware, and software resources) are approved and funded in advance.
- Consider engaging with a PFI on a retainer basis so you can quickly bring them in to assist should a breach happen.

Incident Response Phase Timeline:



PHASE 2: IDENTIFY

Identification (or detection) is an ongoing process where you determine whether you've actually been breached by looking for deviations from normal operations and activities.

An organization normally learns that they have been breached in one of four ways:

- The breach is discovered internally (e.g., review of intrusion detection system logs, alerting systems, system anomalies, or anti-malware scan malware alerts).
- Your bank informs you of a possible breach based on reports of customer credit card fraud.
- Law enforcement discovers the breach while investigating the sale of stolen card information.
- A customer complains to you because your organization was the last place they used their card before it began racking up fraudulent charges.

PHASE 3: CONTAIN

When an organization becomes aware of a possible breach, it's understandable to want to fix it immediately.

However, without taking the proper steps and involving the right people, you can inadvertently destroy valuable forensic data. Forensic investigators use this data to determine how and when the breach occurred, as well as help devise a plan to prevent similar future attacks.

When you discover a breach, remember:

- Don't panic.
- Don't make hasty decisions.
- Don't wipe and reinstall your systems (yet).
- Contact your forensic investigator to help you contain the breach.

Steps to consider during containment and documentation:

- Stop the leakage of sensitive data as soon as possible
- Unplug affected systems from the network, rebuild clean new systems, and keep old systems offline. This is the best option if it's possible because it allows a forensic investigator to evaluate untouched systems. This is easier to do in virtual server environments but can be costly.
- If system replacement is not possible, the next main task will be documentation. This means you need to preserve as much information as possible for forensic analysis. If you know how to take a complete image of your system, you should do so. If you know where the virus files are, copy that directory to a backup. Resort to screenshots or phone videos of behaviors as a last resort before taking action to change the systems.
- Call in a professional forensic investigator to help learn about the breach. In some industries, this may be a required step (such as when payment data is stolen), but it's always recommended to get forensic analysts involved, so you can develop better future processes.

PHASE 4: ERADICATE

After containing the incident, you need to find and remediate the policies, procedures, or technology that led to the breach. This means all malware should be securely removed, and systems should again be hardened, patched, and updated.

Whether you do this or bring in a third party to help you, it's important to be thorough. If any security issues or traces of malware remain in your systems, you may still be losing sensitive data (with your liability increasing).

Set your incident response plan into motion immediately after learning about a suspected data breach.

PHASE 5: RECOVER

Recovering from a data breach is the process of restoring and returning affected systems and devices back into your business environment. During this time, it's important to get your systems and business operations up and running again as quickly as possible.

Remember to ensure all systems have been hardened, patched, replaced, and tested before you consider reintroducing the previously compromised systems back into your production environment.

PHASE 6: REVIEW

After the forensic investigation, meet with all incident response team members and discuss what you've learned from the data breach, reviewing the events in preparation for future attacks.

This is where you will analyze everything about the data breach. Determine what worked well and what didn't in your response plan. Then, revise your plan.

What To Include In An Incident Response Plan

Creating an incident response plan can seem overwhelming. To simplify the process, develop your incident response plan in smaller, more manageable procedures.

While every organization needs varying policies, training, and documents, there are a few itemized response lists that most organizations should include in their incident response plan, such as:

- Emergency contact/communications list
- System backup and recovery processes list
- Forensic analysis list
- Jump bag list
- Security policy review list

**Never Have
a False Sense
of Security.™**

**Learn More About
SecurityMetrics
PCI DSS Audits.**

[Learn More](#)

EMERGENCY CONTACT/ COMMUNICATIONS LIST

Proper communication is critical to successfully managing a data breach, which is why you need to document a thorough emergency contact/communications list. Your list should contain information about: who to contact, how to reach these contacts, the appropriate timelines to reach out, and what should be said to external parties.

In this list, you should document everyone that needs to be contacted in the event of a data breach, such as the following individuals:

- Response team
- Executive team
- Legal team
- Forensics company
- Public relations
- Affected individuals
- Law enforcement
- Merchant processor

You need to determine how and when notifications will be made. Several states have legislated mandatory time frames that dictate when an organization must make notifications to potentially affected cardholders and law enforcement. You should be aware of the laws in your state and have instructions in your incident response plan that outline how you will make mandated notifications.

Your incident response team should craft specific statements that target the various audiences, including a holding statement, press release, customer statement, and internal/employee statement. For example, you should have prepared emails and talking points ready to go after a data breach.

Your statements should address questions like:

- Which locations were and are impacted by the breach?
- How was the breach discovered?
- Is any other sensitive data at risk?
- How will it affect customers and the community?
- What services or assistance (if any) will you provide your customers?
- When will you be back up and running?
- What will you do to prevent this from occurring again?

Identify in advance the party within your organization that is responsible for timely notifications that fulfill your state's specific requirements. This could be your inside legal counsel, newly hired breach management firm, or C-level executive.

Your public response to the data breach will be judged heavily, so review your statements thoroughly.

SYSTEM BACKUP AND RECOVERY PROCESSES LIST

Your system backup and recovery processes list will help you deal with the technical aspects of a data breach. Here are some things that should be included:

- Procedures for disconnecting from the Internet (e.g., who is responsible to decide whether or not you disconnect)
- System configuration diagrams that include information like device descriptions, IP addresses, and OS information
- Process for switching to redundant systems and preserving evidence
- Process for preserving evidence (e.g., logs, timestamps)
- Practices to test the full system backup and system recovery
- Steps to test and verify that any compromised systems are clean and fully functional

This list helps you preserve any compromised data, quickly handle a data breach, and preserve your systems through backups. By creating and implementing this list, your organization can lessen further data loss and help you return to normal operations as quickly as possible.

FORENSICS ANALYSIS LIST

A forensics analysis list is for organizations that use in-house forensic investigations resources. Your forensic team will need to know where to look for irregular behavior and how to access system security and event logs. You might need multiple lists based on your different operating systems and functionalities (e.g., server, database).

Your forensic team may need the following tools:

- Data acquisition tools
- Write-blockers
- Clean/wiped USB hard drives
- Cabling for all connections in your environment
- Other forensic analysis tools (e.g., EnCase, FTK, X-Ways)

If your organization doesn't have access to an experienced computer forensic examiner in-house, you will want to consider hiring a forensics firm, vetting them in advance with pre-completed agreements. This vetting process helps ensure you get an experienced forensic investigator when you need it.

JUMP BAG LIST

Your jump bag list is for grab-and-go responses (i.e., when you need to respond to a breach quickly). This list should include overall responses and actions employees need to take immediately after a data breach. Your list will keep your plan organized and prevent mistakes caused by panic.

Some things to include in your jump bag list are:

- Incident handler's journal to document the incident (e.g., who, what, where, when, why)
- Incident response team contact list
- USB hard drives and write-blockers
- USB multi-hub
- Flashlight, pens, notebooks
- All of your documented lists
- USB containing bootable versions of your operating system(s)
- Computer and network tool kit
- Hard duplicators with write-block capabilities
- Forensic tools and software (if you decide to use in-house forensic investigations resources)

SECURITY POLICY REVIEW LIST

Your security policy review list deals with your response to a breach and its aftermath. This list helps you analyze the breach, so you can learn what to change.

Your security policy review list should include documentation of the following things:

- When the breach was detected, by whom and what method
- Scope of the incident and affected systems
- Data that was put at risk How the breach was contained and eradicated
- Work performed and changes made to systems during recovery
- Areas where the response plan was effective
- Areas that need improvement (e.g., which security controls failed, improvements to security awareness programs)

You should look at where your security controls failed and how to improve them. The purpose of this list is to document the entire incident, what was done, what worked, what didn't, and what was learned.

Develop Your Incident Response Plan

Developing and implementing a thorough incident response plan will help your business handle a data breach quickly and efficiently, while also minimizing the damage from a data breach.

STEP 1: IDENTIFY AND PRIORITIZE ASSETS

Start by identifying and documenting where your organization keeps its crucial data assets. Assess what would cause your organization to suffer heavy losses if it was stolen or damaged.

After identifying critical assets, prioritize them according to the importance and highest risk (e.g., risks based on your annual risk assessment), quantifying your asset values. This will help justify your security budget and show executives what needs to be protected and why it's essential to do so.

STEP 2: IDENTIFY POTENTIAL RISKS

Determine what risks and attacks are the greatest current threats against your systems. Keep in mind that these risks will be different for every organization.

For organizations that process data online, improper coding could be their biggest risk. For a brick-and-mortar organization that offers Wi-Fi for their customers, their biggest risk may be improper network access. Some organizations may place a higher priority on ensuring physical security, while others may focus on securing their remote access applications.

Here are examples of a few possible risks:

- **External or removable media:** Malware executed from removable media (e.g., flash drive, CD)
- **Attrition:** Employs brute force methods (e.g., DDoS, password cracking)
- **Web:** Malware executed from a site or web-based app (e.g., drive-by download)
- **Email security:** Malware executed via email message or attachment (e.g., malware)
- **Impersonation:** Replacement of something benign with something malicious (e.g., SQL injection attacks, rogue wireless access points)
- **Loss or theft:** Loss of computing device or media (e.g., laptop, smartphone)

STEP 3: ESTABLISH PROCEDURES

If you don't have established procedures to follow, a panicked employee may make detrimental security decisions that could damage your organization.

Your data breach policies and procedures should include:

- A baseline of normal activity to help identify breaches
- How to identify and contain a breach
- How to record information on the breach
- Notification and communications plan
- Defense approach
- Employee training

Over time, you may need to adjust your policies according to your organization's needs. Some organizations might require a more robust notification and communication plan, while others might need help from outside resources. However, all organizations need to focus on employee training (e.g., your security policies and procedures).

STEP 4: SET UP A RESPONSE TEAM

Organize an incident response team that coordinates your organization's actions after a data breach.

Your team's goal should be to coordinate resources during a security incident to minimize impact and restore operations as quickly as possible.

Some of the necessary team roles are:

- Team leader
- Lead investigator
- Communications leader
- C-suite representative
- IT director
- Public relations
- Documentations and timeline leader
- Human resources
- Legal representative
- Breach response experts

Make sure your response team covers all aspects of your organization and understand their particular roles in the plan. Each member will bring a unique perspective to the table, and they should own specific data breach response roles that are documented to manage a crisis.

STEP 5: SELL THE PLAN

Your incident response team won't be effective without proper support and resources to follow your plan.

Security is not a bottom-up process. Management at the highest level (e.g., CEO, VP, CTO) must understand that security policies—like your incident response plan—must be implemented from the top and pushed down. This is true for both enterprise organizations as well as mom-and-pop shops.

For enterprise organizations, executive members need to be on board with your incident response team. For smaller organizations, management needs to support additional resources planned for incident response.

When presenting your incident response plan, focus on how your plan will benefit your organization (e.g., financial and brand benefits). For example, if you experience a data breach and manage the incident poorly, your company's reputation will likely receive irreparable brand damage.

The more effective you are at presenting your goals, the easier it will be to obtain necessary funding to create, practice, and execute your incident response plan.

STEP 6: TRAIN YOUR STAFF

Just having an incident response plan isn't enough. Employees need to be properly trained on your incident response plan and know what they're expected to do after a data breach. This means training your team on a regular basis to ensure they know how to respond.

The regular work routine makes it easy for staff to forget crucial security lessons and best practices.

Employees also need to understand their role in maintaining company security. To help them, teach employees to identify attacks such as phishing emails, spear phishing attacks, and social engineering efforts.

Test Your Incident Response Plan

To help staff, regularly test their reactions through real-life simulations such as tabletop exercises. Tabletop exercises allow employees to learn and practice their incident response roles when nothing is at stake, which can help you discover gaps in your incident response plan (e.g., communication issues).

TYPES OF TABLETOP EXERCISES

DISCUSSION-BASED EXERCISE

In a discussion-based tabletop exercise, incident response team members discuss response roles in hypothetical situations. This tabletop exercise is a great starting point because it doesn't require extensive preparation or resources, while it still tests your team's response to real-life scenarios without risk to your organization.

However, this exercise can't fully test your incident response plan or your team's response roles.

SIMULATION EXERCISE

In a simulation exercise, your team tests their incident responses through a live walk-through test that has been highly choreographed and planned. This exercise allows participants to experience how events actually happen, helping your team better understand their roles.

However, simulation exercises require a lot of time to plan and coordinate, while still not fully testing your team's capabilities.

PARALLEL TESTING

In parallel testing, your incident response team actually tests their incident response roles in a test environment. Parallel testing is the most realistic simulation and provides your team with the best feedback about their roles.

Parallel testing is more expensive and requires more time planning than other exercises because you need to simulate an actual production environment, with realistic systems and networks.

CONDUCT A TABLETOP EXERCISE

Before conducting a tabletop exercise, determine your organization's needs by asking:

- Has your incident response team received adequate training regarding their roles and responsibilities?
- When did you last conduct a tabletop exercise?
- Have there been recent organizational changes that might affect your incident response plan?
- Has there been any recent guidance or legislation that might impact your response plan?

Next, design your tabletop exercise around an incident response plan topic or section that you want tested. Identify any desired learning objectives or outcomes. From there, create and coordinate with your tabletop exercise staff (e.g., facilitator, participants, and data collector) to schedule your tabletop exercise.

When designing your tabletop exercise, prepare the following exercise information in advance:

- A **facilitator guide** that documents your exercise's purpose, scope, objective, and scenario, including a list of questions to address your exercise's objectives.
- A **participant briefing** that includes the exercise agenda and logistics information.
- A **participant guide** that includes the same information as the facilitator guide, except it either doesn't include any of the questions or includes a shorter list of questions designed to prepare participants.
- An **after-action report** that documents the evaluations, observations, and lessons learned from your tabletop exercise staff.

After conducting a tabletop exercise, set up a debrief meeting to discuss response successes and weaknesses.

Your team's input will help you know where and how to make necessary revisions to your incident response plan and training processes.



Data Breach Prevention Tools

This section outlines data breach prevention tools that can help improve your data breach response and increase your data security.

INSTALL AND MONITOR FILE INTEGRITY MONITORING SOFTWARE

File integrity monitoring (FIM) software is a great companion for your malware prevention controls. New malware comes out so frequently you can't just rely on anti-virus software to protect your systems. It often takes many months for a signature of newly detected malware to make it into the malware signature files, which allows it to be detected by anti-virus software.

Configure FIM software to watch critical file directories for changes. FIM software is typically configured to monitor areas of a computer's file system where critical files are located. FIM tools will generate an alert that can be monitored when a file is changed.

Malware is software that consists of files that are copied to a target computer. Even if your anti-virus software cannot recognize the malware files' signatures, FIM software will detect that files have been written to your computer and will alert you to check and make sure you know what those files are. If the change was known (like a system update), then you don't need to worry. If not, chances are you have new malware added that could not be detected and can now be dealt with.

Here are some places where FIM should be set up to monitor:

- Operating system critical directories
- Critical installed application directories
- Web server and/or web application directories
- User areas (if an employee facing computer)

FIM can also be set up to check if web application code or files are modified by an attacker.

INSTALL INTRUSION DETECTION AND PREVENTION SYSTEMS

One of the reasons data breaches are so prevalent is a lack of proactive, comprehensive security dedicated to monitoring system irregularities, such as intrusion detection systems (IDS) and intrusion prevention systems (IPS).

Using these systems can help identify a suspected attack and help you locate security holes in your network that attackers used. Without the knowledge derived from IDS logs, it can be very difficult to find system vulnerabilities and determine if cardholder data was accessed or stolen.

By setting up alerts on an IDS, you can be warned as soon as suspicious activity is identified and be able to significantly minimize compromise risk within your organization. You may even stop a breach in its tracks.

An IDS could help you detect a security breach as it's happening in real time.

For more preventive measures, you might consider an IPS, which also monitors network activity for malicious activities, logs this information, and reports it; but it can prevent and block many intrusions that are detected. An IPS can drop malicious packets, block traffic from the malicious source address, and reset connections.

INSTALL DATA LOSS PREVENTION SOFTWARE

In addition to these, you should have data loss prevention (DLP) software in place. DLP software watches outgoing data streams for sensitive or critical data formats that should not be sent through a firewall, and it blocks this data from leaving your system.

Make sure to properly implement it, so that your DLP knows where data is allowed to go, since if it's too restrictive, it might block critical transmissions to third party organizations.



Conclusion

SECTION CONTENTS

PCI DSS Budget	131	Contributors	136
Create A Security Culture	133	Terms And Definitions	137

PCI DSS Budget

The cost of PCI compliance depends on your organization's structure. Here are a few variables that will factor into the cost of your overall compliance to the PCI DSS:

- **Your business type (e.g., franchise, service provider, mom-and-pop shop):** Each business type will have varying amounts of transactions, cardholder data, environment structure, risk levels, and merchant or service provider levels, meaning that each business will have different security requirements.
- **Your organization's size:** Typically, the larger the organization, the more potential vulnerabilities it has. More staff members, more programs, more processes, more computers, more cardholder data, and more departments mean more cost.
- **Your organization's environment:** The type of processing systems, the brand of computers, the kind of firewalls, the model of back-end servers, etc. can all affect your PCI cost.
- **Your organization's dedicated PCI staff and outside help:** Even with a dedicated team, organizations usually require outside assistance or consulting to help them meet PCI requirements.

The following are estimated annual PCI budgets:¹²

SMALL ENTITY BUDGET	
Self-assessment questionnaire (SAQ)	\$50 – \$200
Vulnerability scan	\$100 – \$150 (PER IP ADDRESS)
Training and policy development	\$70 (PER EMPLOYEE)
Total possible cost:	\$220+

MEDIUM/LARGE ENTITY BUDGET	
Onsite audit	\$40,000+
Vulnerability scan	\$800+
Penetration testing	\$15,000+
Training and policy development	\$5,000+
Total possible cost:	\$60,800+

Keep in mind this budget doesn't include implementing and managing security controls, such as firewalls, encryption, and updating systems and equipment.

Create A Security Culture

Unless someone oversees PCI on management's side (not just IT), PCI compliance won't happen. We often see departments inside companies (e.g., networking, IT, HR, risk) expecting other departments to take charge of PCI compliance, which means nobody is in charge of it. Other times, organizations expect a third-party QSA to be the PCI project manager, which is not feasible because the QSA's role is to assess what is in place, not create a security and compliance program.

Security is not a bottom-up process. Management often says or implies that IT should "just get their organization secure." However, those placed in charge of PCI compliance and security may not have the means necessary to reach their goals.

For example, IT may not have the budget to implement adequate security policies and technologies (e.g., firewalls, FIM). Some may try to look for free software to fill in security gaps, but this process can be expensive due to the time it takes to implement and manage. In some instances, we have seen IT departments wanting their PCI auditor to purposely fail their compliance evaluations so they could prove their higher security budget needs. Obviously, it would have been better to focus on security from the top level down beforehand.

C-level management should support the PCI process. If you are a C-level executive, you should be involved with budgeting, assisting, and establishing a security culture from the top-down.

Additionally, organizations can sometimes focus on becoming "certified" as PCI compliant, while not actually addressing, monitoring, and regularly reviewing critical security controls and processes. Keep in mind that this attitude of just checking off SAQ questions doesn't make an organization PCI compliant, nor will it protect them from future data breaches.

OVERCOME MANAGEMENT'S BUDGET CONCERNS

If you're having problems communicating budgetary needs to management, conduct a risk assessment before starting the PCI process. NIST 800-30 is a good risk assessment protocol to follow. At the end of your assessment, you'll have an idea of your compromise probability, how much a compromise would cost, and the impact a breach might have on your organization (including brand damage).

Simply put, you need to find a way to show how much money weak security will cost the organization. For example, "if someone gains access to the system through X, this is how much it will cost and how much damage it will cause." Consider asking marketing or accounting teams for help delivering the message in more bottom-line terms.

If possible, work with a QSA to identify security controls to address what tools you may need to implement.

PCI DSS Responsibilities and Challenges



JEN STONE

SecurityMetrics Senior Security Analyst
CISSP | CISA | QSA | CCSFP | CHQP

In my experience, small merchants and service providers tend to struggle with documenting and following policies and procedures. During a PCI DSS assessment, a QSA will verify that required policies and procedures are in place and being followed.

Smaller merchants and service providers whose CDE consists of only a few machines often feel that they don't have time to document procedures. Unfortunately, it's not uncommon to perform a renewal assessment where the business neglected to maintain compliance due to employee turnover and lack of documentation.

At a minimum, small merchants should set up a PCI email user or active directory account and add reminders in their calendar to perform security processes throughout the year (e.g., quarterly vulnerability assessment scans, semi-annual firewall reviews). The evidence collected from these tasks can then be sent to that PCI

account for storage. This is a low-cost solution that can help key personnel keep PCI DSS compliance on their minds throughout the year. It will also help document necessary evidence for their annual self-assessment (or to their assessor).

Large enterprise organizations usually document their policies and procedures sufficiently. They generally have very specific and thorough change control processes, and they typically follow documented approval processes prior to implementing changes to their CDE. Unfortunately, due to their size and the different entities involved in their CDE management, their reaction time tends to be much slower, with different stakeholders often making contradictory decisions. When vulnerability scans or penetration tests identify weaknesses that may place their CDE at risk, it's not always apparent which group should be responsible for addressing these vulnerabilities.

Small merchants and service providers tend to struggle with documenting and following policies and procedures.

To help address some of these concerns, requirement 12 details how service providers need to define a charter for the organization's compliance program, involving executive management. While this is only required for service providers, it's recommended that larger merchants follow this requirement as well.

Large organizations and service providers should establish an official PCI charter that describes the management and accountability of the organization's compliance program.³ Additionally, they should implement internal audit procedures to ensure security practices are properly in place throughout the year.³

PCI compliance cannot just be an annual audit event.

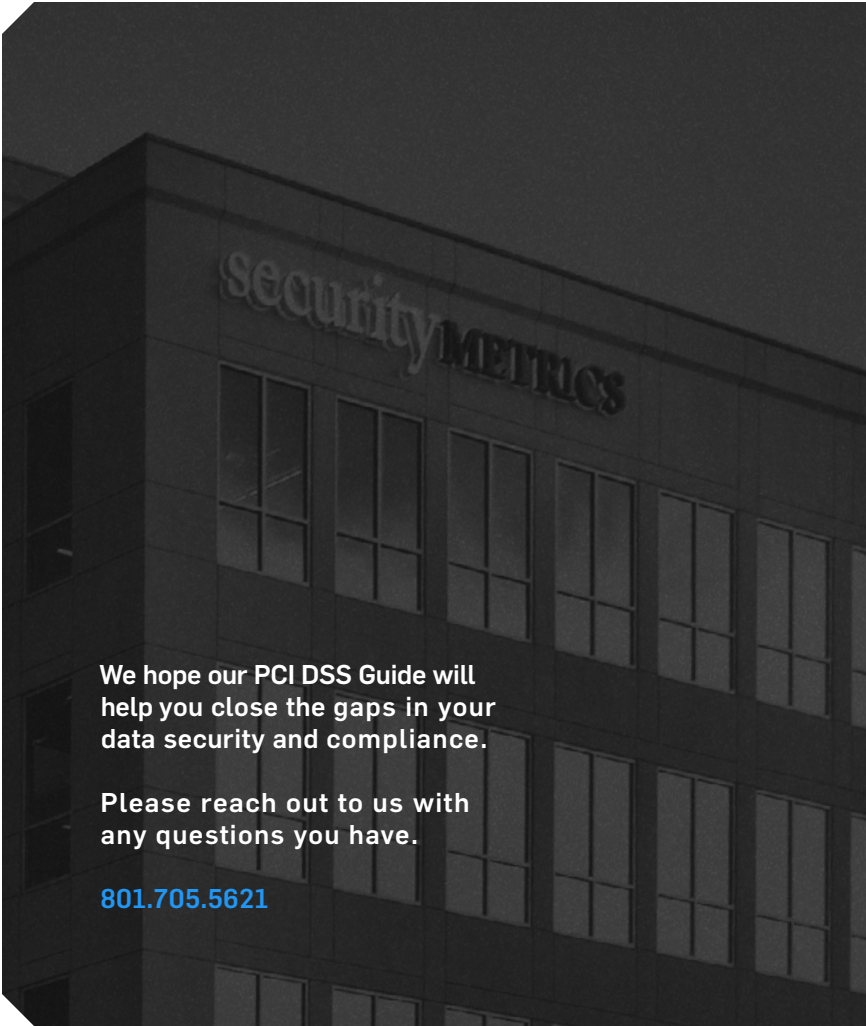
Often, organizations are not leveraging many of the PCI requirements in a way that actually increases security for their CDE.

For instance, PCI requires log centralization and daily reviews. PCI also requires change detection or FIM on CDE systems to detect unauthorized changes to key files and directories. To achieve compliance, organizations might set up log monitoring and FIM, but then ignore every alert coming their way. They may technically have FIM and log monitoring in place, but these systems alone are not making their environments more secure because necessary time and effort are not taken to respond to genuine alerts.

As you implement your cybersecurity program, make sure you understand why a security control is required so you can structure tools and processes around the protection each control offers.

Contributors

Matt Halbleib	Brad Caldwell
Jen Stone	Joshua Brandeberry
Michael Simpson	Jeff Compton
Gary Glover	Heather Page
Michael Maughan	Chuck Brailsford
Winn Oakey	Matt Goodman
David Page	Rich Bushell
Michael Ohran	Jon Clark
Trevor Hansen	Sarah Kemple
Mark Miner	Jameson Olsen
Winnie Miller	Hunter Steffen
Marj Eldard	Katherine Bullock
David Ellis	Emory French-Folsom
Aaron Willis	Ashley Perry
Bradley Smith	Karen Smith
Chandler Loveland	Ben Caldwell
Brad Nelson	Eric Smith



We hope our PCI DSS Guide will help you close the gaps in your data security and compliance.

Please reach out to us with any questions you have.

[801.705.5621](tel:801.705.5621)

Terms And Definitions

Access Control List (ACL): A list of instructions for firewalls to know what to allow in and out of systems.

Advanced Encryption Standard (AES): A government encryption standard to secure sensitive electronic information.

Approved Scanning Vendor (ASV): A company approved by the PCI SSC to conduct vulnerability scanning tests.

Captured: Data is being recorded, gathered, or stored from an unauthorized source.

Card Verification Value (CVV/CSC/CVC/CAV): Element on a payment card that protects information on the magnetic stripe. Specific acronyms depend on the card brand.

Cardholder Data Environment (CDE): Any individual, software, system, or process that processes, stores, or transmits cardholder data.

Cardholder Data (CHD): Sensitive data found on payment cards, such as an account holder name or PAN data.

Chief Information Security Officer (CISO): Similar to a CSO, but with responsibility for IT rather than entity-wide security.

Data Loss Prevention (DLP): A piece of software or strategy used to catch unencrypted data sent outside the network.

Domain Name Server (DNS): A way to translate URLs to IP addresses.

Exfiltrated: The unauthorized transfer of data from a system.

Federal Information Processing Standards (FIPS): US federal government standards for computer security that are publicly announced (e.g., encryption standards).

File Integrity Monitoring (FIM): A method to watch for changes in software, systems, and applications to detect potential malicious activity.

File Transfer Protocol (FTP): An insecure way to transfer computer files between computers using the Internet. (See *SFTP*)

Firewall (FW): A system designed to screen incoming and outgoing network traffic.

Hypertext Transfer Protocol (HTTP): A method of communication between servers and browsers. (See *HTTPS*)

Hypertext Transfer Protocol Over Secure Socket (HTTPS): A secure method of communication between servers and browsers. (See *HTTP*)

Incident Response Plan (IRP): Policies and procedures to effectively limit the effects of a security breach.

Information Technology (IT): Anything relating to networks, computers, and programming, including the people that work with those technologies.

Internet Protocol (IP): Defines how computers send packets of data to each other.

Intrusion Detection System (IDS): Types of systems that are used to monitor network traffic and report potential malicious activity.

Intrusion Prevention System (IPS): Types of systems that—like an IDS—monitors network traffic and reports potential malicious activity, but also prevents and blocks many detected.

Multi-factor Authentication (MFA): Two out of three independent methods of authentication are required to verify a computer or network user. The three possible factors are:

- Something you *know* (such as a username and password)
- Something you *have* (such as an RSA token or one-time password token)
- Something you *are* (such as fingerprint or iris scans)

National Institute of Standards and Technology (NIST): Federal technology agency that assists in developing and applying technology, measurements, and standards (e.g., the NVD).

National Vulnerability Database (NVD): A repository of all known vulnerabilities, maintained by NIST.

Network Access Control (NAC): Restricts data that users, apps, and programs can access on a computer network.

Open Web Application Security Project (OWASP): A non-profit organization focused on software security improvement. Often heard in the context of “OWASP Top 10”—a list of top threatening vulnerabilities.

Payment Card Industry Data Security Standard (PCI DSS): Requirements put together by the PCI SSC, required of all businesses that process, store, or transmit payment card data to help prevent cardholder data theft.

Payment Card Industry Security Standards Council (PCI SSC): An organization established in 2006 by Visa, MasterCard, American Express, Discover Financial Services, and JCB International to regulate cardholder data security.

Point-To-Point Encryption (P2PE): Payment card data encryption from the point of interaction to a merchant solution provider.

Primary Account Number (PAN): The 12 to 19 digits that identify a payment card. Also called a bank card number or payment card number.

Qualified Security Assessor (QSA): Individuals and firms certified by the PCI SSC to perform PCI compliance assessments.

Risk: The likelihood that a threat will trigger or exploit a vulnerability and the resulting impact on an organization.

Risk Assessment (RA): An assessment of the potential vulnerabilities, threats, and possible risk to the confidentiality, integrity, and availability of payment data held by an organization.

Risk Management Plan (RMP): The strategy to implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level.

Role-Based Access Control (RBAC): The act of restricting users' access to systems based on their role within an organization.

Secure File Transfer Protocol (SFTP): A secure way to encrypt data that is in transit. (See FTP)

Secure Socket Layer (SSL): An outdated Internet security standard for encrypting the link between a website and a browser to enable transmission of sensitive information (predecessor to TLS).

Self-Assessment Questionnaire (SAQ): A collection of questions used to document an entity's PCI DSS assessment results, based on their processing environment.

Threat: The potential for a person, event, or action to exploit a specific vulnerability.

Transport Layer Security (TLS): A more secure Internet security standard for encrypting the link between a website and a browser to enable transmission of sensitive information. (See *SSL*)

Two-Factor Authentication (TFA): (See *MFA*)

Virtual Private Network (VPN): A strategy of connecting remote computers to send and receive data securely over the Internet as if they were directly connected to the private network.

Vulnerability: A flaw or weakness in procedure, design, implementation, or security control that could result in a security breach.

Vulnerable: A state in which a weakness in a system, environment, software, or website could be exploited by an attacker.

Web Application Firewall (WAF): An application firewall that monitors, filters, and blocks HTTP traffic to and from a web application.

Wi-Fi Protected Access (WPA): A security protocol designed to secure wireless computer networks. (See *WPA2*)

Wi-Fi Protected Access II (WPA2): A more secure version of WPA. (See *WPA*)

Wired Equivalent Privacy (WEP): An outdated and weak security algorithm for wireless networks.

Wireless Local Area Network (WLAN): A network that links to two or more devices wirelessly.

Appendix

1. PCI Security Standards Council, LLC (2022). *The prioritized approach to pursue PCI DSS compliance* [webpage]. Retrieved from <https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/Prioritized-Approach-For-PCI-DSS-v4-0.pdf>
2. PCI Security Standards Council, LLC (2016). *Information supplement: Guidance for PCI DSS scoping and network segmentation* [webpage]. Retrieved from https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf
3. PCI Security Standards Council, LLC (2022). Payment card industry (PCI) data security standard: Requirements and testing procedures version 4.0 [webpage]. Retrieved from https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf
4. PCI Security Standards Council, LLC (2022). *List of validated products and solutions* [webpage]. Retrieved from https://www.pcisecuritystandards.org/assessors_and_solutions
5. PCI Security Standards Council, LLC (2018). *PCI data security essentials for small merchants* [webpage]. Retrieved from <https://www.pcisecuritystandards.org/pdfs/PCI-DSE-Overview-for-Small-Merchants.pdf>
6. PCI Security Standards Council, LLC (2022). *Countdown to PCI DSSv4.0* [webpage]. Retrieved from <https://blog.pcisecuritystandards.org/countdown-to-pci-dss-v4.0>
7. PCI Security Standards Council, LLC (2019). *5 questions about PCI DSS v4.0* [webpage]. Retrieved from <https://blog.pcisecuritystandards.org/5-questions-about-pci-dss-v4-0>
8. PCI Security Standards Council, LLC (2018). *Information supplement: Protecting telephone-based payment card data* [webpage]. Retrieved from https://www.pcisecuritystandards.org/documents/Protecting_Telephone_Based_Payment_Card_Data_v3-0_nov_2018.pdf
9. SecurityMetrics (2023). *PANscan trends* [webpage]. Retrieved from <https://www.securitymetrics.com/learn/panscan-trends>
10. PCI Security Standards Council, LLC (2017). *Information supplement: Multi-factor authentication* [webpage]. Retrieved from <https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf>
11. Glover, G. (2022). *How much does PCI compliance cost?* [webpage]. Retrieved from <https://www.securitymetrics.com/blog/how-much-does-pci-compliance-cost>
12. PCI SecurityStandards Council, LLC (2019). Payment card industry (PCI) point-to-point encryption: P2PE instruction manual (PIM) template [webpage]. Retrieved from https://www.pcisecuritystandards.org/documents/P2PE_v3.0_PIM_Template.docx

Our Products and Services



1. PCI Compliance:

- PCI for Small Business
- PCI Policies
- PCI Training
- PCI DSS Audit
- SSF Audit
- P2PE Audit

2. HIPAA Compliance:

- HIPAA for Small Business
- HIPAA Policies
- HIPAA Training
- HIPAA Audit

3. GDPR Compliance:

- GDPR Defense
- GDPR Assessment

4. Managed Programs:

- PCI compliance Program for PCI Level 1-4 Merchants
- HIPAA for Health Networks

5. Vulnerability Scanning:

- External Vulnerability Scan
- Internal Vulnerability Scan
- Mobile Security

6. Data Discovery:

- Card Data Discovery
- PII Data Discovery

7. Ecommerce Security:

- Shopping Cart Inspect
- Shopping Cart Monitor

8. Security Operations:

- SecurityMetrics Pulse SOS
- Antivirus Essentials

9. Workforce Training:

- Security and Compliance Training
- Cybersecurity Training
- PCI Security Training
- HIPAA Security and Privacy Training
- Policies and Procedures Templates

10. Security Audits:

- EI3PA Compliance
- NIST 800-30 Risk Assessment
- CIS Controls
- PIN Security Assessment
- Security Consulting
- HITRUST

11. Security Testing:

- Penetration Testing

12. Incident Response:

- Incident Response
- Table Top Exercises

ABOUT SECURITYMETRICS

We secure peace of mind for organizations that handle sensitive data. We hold our tools, training, and support to a higher, more thorough standard of performance and service.

We are a PCI certified Approved Scanning Vendor (ASV), Qualified Security Assessor (QSA), Certified Forensic Investigator (PFI), and Managed Security provider with over 20 years of data security experience. From local shops to some of the world's largest brands, we help all businesses achieve data security through managed services and compliance mandates (PCI, HIPAA, GDPR, HITRUST). We have tested over 1 million systems for data security and compliance. We are privately held and are headquartered in Orem, Utah, where we maintain a Security Operations Center (SOC) and 24/7 multilingual technical support.

www.securitymetrics.com/pci

Looking for a
PCI compliance
solution?

Learn more at:
www.securitymetrics.com/pci



securityMETRICS®