
2019
SecurityMetrics Guide to
PCI DSS Compliance
A Resource for Merchants and Service Providers to Become Compliant
securityMETRICS®

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, including auditors' best practices and IT checklists. Rather than reading this guide cover to cover, we recommend using it as a resource for your PCI compliance efforts.

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

MATT HALBLEIB

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

INTRODUCTION

HOW TO READ THIS GUIDE

Whether you're a new employee with limited PCI knowledge or an experienced system administrator, our guide aims to help you secure your environment and for your organization to become compliant with PCI DSS requirements. We specifically 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.

The chart below displays an overview of the PCI Security Standards Council's Prioritized Approach. 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):

MILESTONES	GOALS
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 card applications
4	Monitor and control access to your systems
5	Protect stored cardholder data
6	Finalize compliance efforts, and ensure all controls are in place

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.

PCI DSS REQUIREMENTS	MILESTONES					
	1	2	3	4	5	6
Requirement 1: Protect Your System with Firewalls	●	●				●
Hardware firewalls		●				
Software firewalls		●				
Properly configure firewalls		●				●
Network segmentation		●				
Test and monitor configuration						●
Requirement 2: Use Adequate Configuration Standards		●	●			
Default password weaknesses		●				
System hardening			●			
System configuration management		●	●			
Requirement 3: Secure Cardholder Data	●				●	
Cardholder data trends	●				●	
Know where all cardholder data resides	●				●	
Requirement 4: Secure Data Over Open and Public Networks		●				
Stop using SSL/early TLS		●				
Requirement 5: Protect Systems with Anti-Virus		●				
Regularly update your anti-virus		●				
Requirement 6: Update Your Systems			●			●
Regularly update and patch system(s)			●			●
Establish software development processes			●			●
Web application firewalls			●			

Requirement 7: **Restrict Access**				●		
Restrict access to cardholder data and systems				●		
Requirement 8: **Use Unique ID Credentials**		●		●		
Weak passwords and usernames		●		●		
Implement multi-factor authentication		●				
Requirement 9: **Ensure Physical Security**	●	●			●	
Control physical access to your workplace		●			●	
Keep track of POS terminals		●				
Train employees early and often		●			●	
Physical security best practices	●	●			●	
Requirement 10: **Implement Logging and Log Management**				●		
System logs and alerting				●		
Establishing log management				●		
Log management system rules				●		
Requirement 11: **Conduct Vulnerability Scans and Penetration Testing**		●		●		
Understand your environment		●		●		
Vulnerability scanning basics		●				
Penetration testing basics		●				
Vulnerability scanning vs. penetration testing		●				
Requirement 12: **Start Documentation and Risk Assessments**	●	●				●
Regularly 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, 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 protecting 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.

SecurityMetrics research concluded that the average breached organization at the time of data compromise was not compliant with at least 44% of the PCI DSS requirements.

None of the organizations SecurityMetrics investigated in 2018 were found to be fully PCI DSS compliant at the time they experienced a data breach.

PCI DSS REQUIREMENTS OVERVIEW

REQUIREMENT 1: PROTECT YOUR SYSTEM WITH FIREWALLS

- Install a hardware and software firewall
- Tweak firewall configuration for your system
- Have strict firewall rules

REQUIREMENT 2: USE ADEQUATE CONFIGURATION STANDARDS

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

REQUIREMENT 3: PROTECT STORED DATA

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

REQUIREMENT 4: SECURE DATA OVER OPEN AND PUBLIC NETWORKS

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

REQUIREMENT 5: PROTECT SYSTEMS WITH ANTI-VIRUS

- Create a vulnerability management plan
- Regularly update anti-virus
- Maintain an up-to-date malware program

REQUIREMENT 6: UPDATE YOUR SYSTEMS

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

REQUIREMENT 7: RESTRICT ACCESS

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

REQUIREMENT 8: USE UNIQUE ID CREDENTIALS

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

REQUIREMENT 9: ENSURE PHYSICAL SECURITY

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

REQUIREMENT 10: IMPLEMENT LOGGING AND LOG MONITORING

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

REQUIREMENT 11: CONDUCT VULNERABILITY SCANS AND PENETRATION TESTING

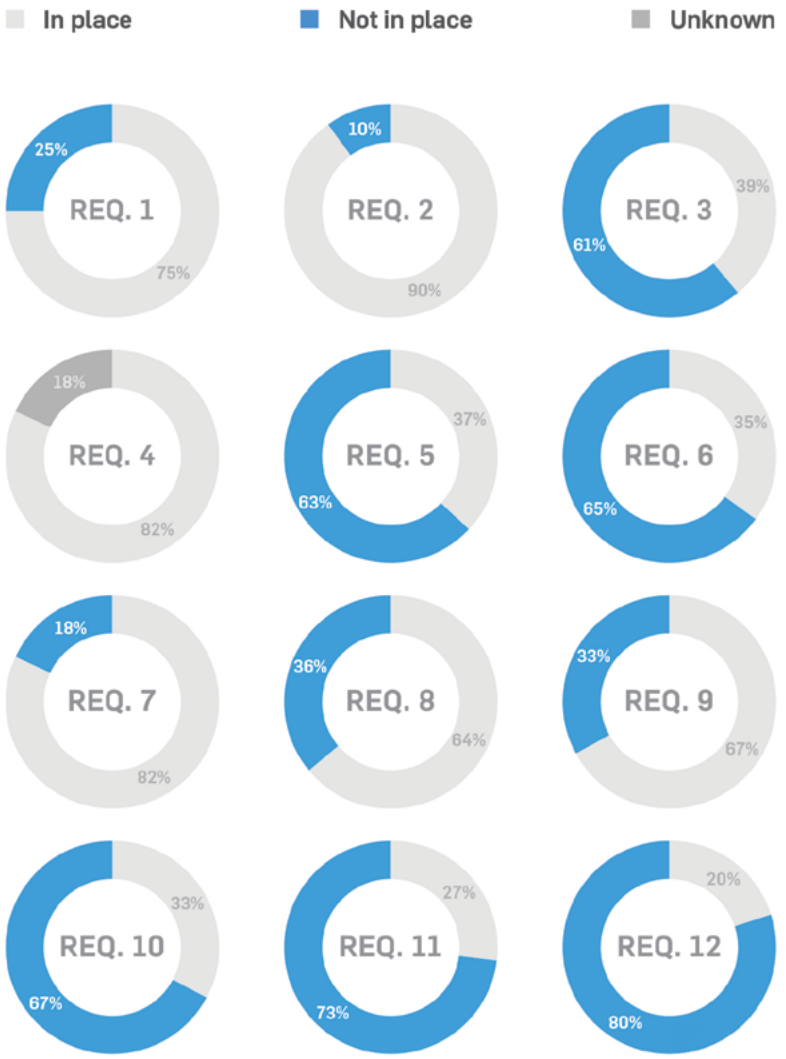
- Know your environment
- Run vulnerability scans quarterly
- Conduct a penetration test

REQUIREMENT 12: START DOCUMENTATION AND RISK ASSESSMENTS

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

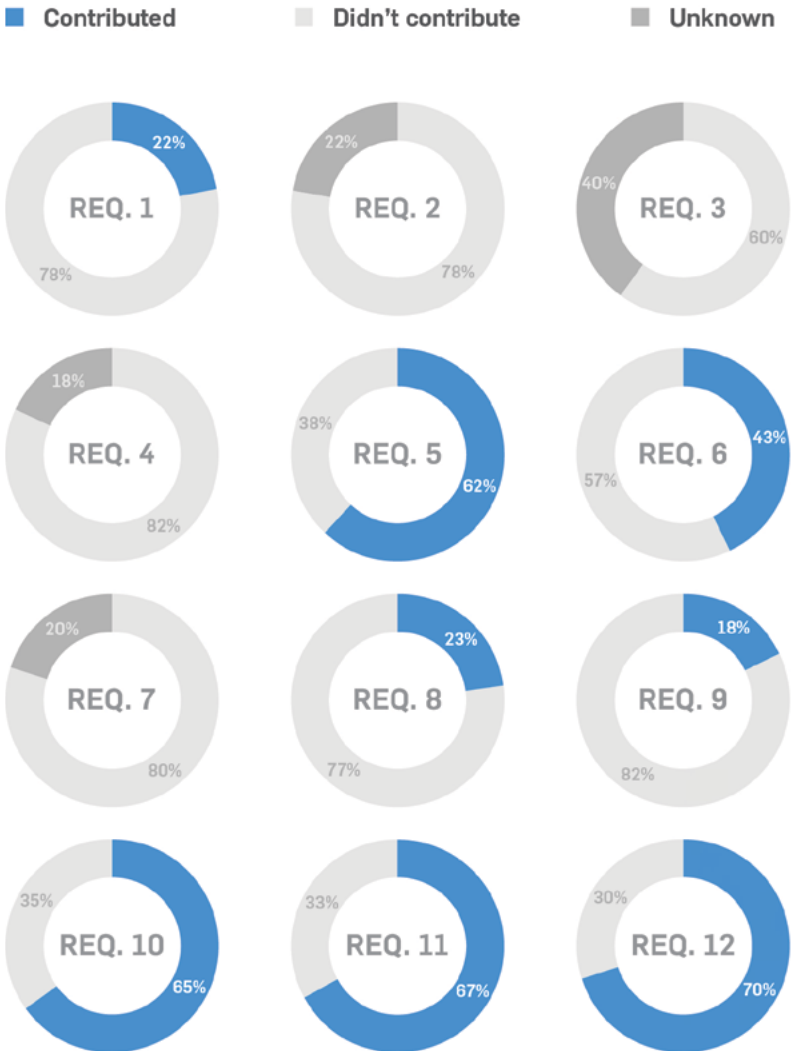
PCI DSS REQUIREMENTS IMPLEMENTED AT THE TIME OF COMPROMISE

The following graphs demonstrate the compliance of compromised businesses we investigated noting whether each requirement was in place at the time of compromise or not in 2018:



NON-COMPLIANCE CONTRIBUTED TO DATA BREACH

The following graphs detail how non-compliance to the different PCI requirements affected breaches for compromised organizations we investigated in 2018:



TOP 10 FAILING SELF-ASSESSMENT QUESTIONNAIRE (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. **Requirement 12.1:** Establish, publish, maintain, and disseminate a security policy.
2. **Requirement 12.6.1:** Educate personnel [with security awareness training] upon hire and at least annually.
3. **Requirement 12.5.3:** Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
4. **Requirement 12.10.1:** Create an incident response plan to be implemented in the event of system breach.
5. **Requirement 12.1.1:** Review the security policy at least annually and update the policy when the environment changes.
6. **Requirement 12.4:** Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
7. **Requirement 12.8.5:** Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.
8. **Requirement 9.9.2:** Periodically inspect device surfaces to detect tampering (e.g., addition of card skimmers to devices), or substitution (e.g., by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).
9. **Requirement 12.3.5:** [Verify that the usage policies define] acceptable uses of the technology.
10. **Requirement 12.8.4:** Maintain a program to monitor service providers' PCI DSS compliance status at least annually.

TAKEAWAYS

Unfortunately, 2018 showed significant decreases in compliance levels when compared to previous years.

None of the investigated breached organizations in 2018 were found to be compliant with PCI DSS. Furthermore, in nearly every case, the vulnerabilities that attackers leveraged to gain access to merchant systems were covered by specific sections of the PCI DSS.

In other words, had the organization been compliant with those sections of the PCI DSS, the breach likely would not have occurred.

UNDERSTANDING YOUR PCI DSS RESPONSIBILITY

PCI DSS 3.2.1 introduced several changes, including changes to PCI scope definitions and SAQ categories. 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 (or is connected to systems that do), 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 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.

85% of SecurityMetrics customers who started their SAQ went on to complete it and achieve a passing status in 2018.

PCI DSS SCOPING AND NETWORK SEGMENTATION SUPPLEMENT

In December 2016, the PCI Security Standards Council (SSC) released a supplemental guide for scoping and network segmentation. 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 or connected to the cardholder data environment (CDE), which is "comprised of people, processes, and technologies that store, process, or transmit CHD or sensitive authentication data."

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:

- Host-based 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.

TIPS FROM AN AUDITOR

PCI DSS SCOPE

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 December 2016, the council released an informational supplement regarding PCI scoping. 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!

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 PCI scope.

Paper trails of hand-written information or photocopied payment card data can sometimes fill multiple rooms. Even if card data is 10 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 back-ups 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.

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

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.

MATT HALBLEIB
QSA (P2PE) | PA-QSA (P2PE) | CISSP

PCI DSS 3.2.1 SAQ TYPES

SAQ	DESCRIPTION	# OF ?S	VULN. SCAN
A	E-commerce 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	22	No
A-EP	E-commerce website (direct post) • Merchant website accepts payment using direct post or transparent redirect service	191	Yes
B	Processes cards via: • Analog phone, fax, or stand-alone terminal • Cellular phone (voice), or stand-alone terminal • Knuckle buster/imprint machine	41	No
B-IP	Processes cards via: • Internet-based stand-alone terminal isolated from other devices on the network	82	Yes
C-VT	Processes cards: • One at a time via keyboard into a virtual terminal • On an isolated network at one location • No swipe device	79	No
C	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	160	Yes
D	E-commerce 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 (email, e-fax, recorded calls, etc.)	329	Yes
P2PE	Point-to-point encryption • Validated PCI P2PE hardware payment terminal solution only • Merchant specifies they qualify for the P2PE questionnaire	33	No

SAQ OVERVIEW

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 (e-commerce or mail/telephone-order) transactions.
- All processing of cardholder data is entirely outsourced to a PCI DSS validated third-party service providers.
- 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 confirmed that all third party(s) handling storage, processing, and transmission of cardholder data are PCI DSS compliant.
- Any cardholder data your company retains is on paper (such as, printed reports or receipts), and these documents are not received electronically.

SAQ A-EP

- Your company only accepts e-commerce 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 e-commerce 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.

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.

SAQ B-IP

- Your business only uses standalone, PTS-approved 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.

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 via direct physical interaction with the payment card.
- 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.

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.

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.

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:

- E-commerce 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 e-commerce environment/website or control the flow of e-commerce data.

PCI DATA SECURITY ESSENTIALS EVALUATIONS FOR SMALL MERCHANTS

This past year, the PCI council released a new 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."

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

PCI DSS 3.2 AND 3.2.1: KEY CHANGES AND UPDATES

PCI DSS 3.2.1 was released on May 17, 2018, replacing version 3.2. PCI DSS 3.2 brought with it some extensive changes, including new requirements for service providers and additional guidance about multi-factor authentication.

The changes from PCI DSS 3.2.1 are characterized by the PCI Council as clarification (as opposed to additional guidance or actual changes in requirements). The intent of clarification from the PCI Council is to ensure that "concise wording in the standard portrays the desired intent of requirements."

USE OF SSL/EARLY TLS

Using SSL/Early TLS encryption for card data transmission poses risks to security since it has many exploitable vulnerabilities.

As of June 30, 2018, SSL/early TLS is no longer an accepted technology for protecting card data in transit. You should now have implemented a more secure encryption protocol such as TLS 1.1 or higher (TLS 1.2 or above is strongly encouraged). The practice of having a risk mitigation plan in place for usage of previous insecure versions will no longer be accepted for PCI DSS compliance.

For merchants still using Point of Sale (POS) Point of Interaction (POI) terminals that utilize SSL and/or early TLS, you need to verify that the terminals (and connected SSL/early TLS termination points) are not susceptible to any known exploits (see appendix A of PCI DSS 3.2.1 for additional requirements). If you are in this situation, it is recommended that you begin a transition plan for upgrading POS/POI terminals to those that support the latest version of TLS.

If you are a service provider that supports POS/POI terminals still using SSL and/or early TLS, then you must have a formal Risk Mitigation and Migration Plan in place until all terminals you support are upgraded to support secure TLS versions. In addition, you must also provide a secure service offering that supports the latest TLS versions (see appendix A of the PCI DSS).

MULTI-FACTOR AUTHENTICATION REQUIRED INTO OR OUT OF THE CDE (8.3)

PCI DSS 3.2.1 evaluates additional multi-factor authentication (MFA) requirements for administrators within a CDE. Multi-factor authentication is an effective way to secure your CDE. To properly configure multi-factor authentication, you must have at least two of three things:

- Something you *know* (e.g., password/passphrase, PIN)
- Something you *have* (e.g., token device, one-time password)
- Something you *are* (e.g., fingerprint scan, retina scan)

Prior to PCI DSS 3.2 and 3.2.1, multi-factor authentication was just required for remote access to the network by employees, administrators, and third parties. But now, even if your connection to the CDE is from an internal network segment, you need to use multi-factor authentication.

As with all PCI DSS requirements, this requirement is a reflection of the current threat landscape. This change helps strengthen security behind your edge firewall as well as outside of it.

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."

MULTI-FACTOR AUTHENTICATION SUPPLEMENT

Last year, the PCI Security Standards Council (PCI SSC) released a supplemental guide on multi-factor authentication, clarifying multi-factor authentication policies. Specifically, the MFA mechanisms should be independent of one another so that access to one factor does not grant access to another. Also, the compromise of any one factor should not affect the integrity or confidentiality of any other factor.

For example, if the same set of credentials (e.g., username/password) is used as an authentication factor and also for gaining access to an e-mail account where a secondary factor (e.g., one-time password) is sent, these factors are not independent. Another faulty example is if you use a software certificate that is stored on a mobile device and protected by the same set of credentials used to log in to that device.

For good MFA implementation, you should include independence of authentication mechanisms and protection of authentication factors. You should also ensure that knowledge of the success or failure of a factor is not provided to the individual until all factors have been submitted.

All non-console administrative access to CDE requires multi-factor authentication.

A common way to implement the independence of authentication factors is through physical separation of these factors. You might also be able to use highly robust and isolated execution environments, such as "trusted execution environment [TEE], Secure Element [SE], and Trusted Platform Module [TPM])."

CLARIFYING MASKING CRITERIA (3.3)

PCI DSS 3.2.1 clarifies masking criteria for when primary account numbers (PAN) are displayed. Masking is described as hiding data from view; this is not the same as encryption. When displaying a credit card number or bank identification number (BIN) outside of your organization, you are allowed to display (at a maximum) the first six and last four numbers. If you include more than this information, you're not compliant.

Additionally, you must have "a list of roles that need access to displays of more than the first six/last four (includes full PAN)." Whether or not you should display fewer PAN numbers could depend on various legal requirements. If your business stores PAN, you're also required to encrypt and properly secure it.

CHANGE MANAGEMENT PROCESS (6.4.6)

PCI DSS 3.2.1 explains that you need to have a change management process in place to ensure that all new or changed systems and networks implement relevant PCI DSS requirements after a significant change. Your documentation should include what qualifies as a significant change and these process updates.

Examples of requirements that could be impacted by significant changes:

- Network diagram is updated to reflect changes.
- Systems are configured according to configuration standards with all default passwords changed and unnecessary services disabled.
- Systems are protected with required system controls (e.g., FIM, anti-virus, patches, audit logging).
- Sensitive authentication data (SAD) is not stored and all cardholder data (CHD) storage is documented and incorporated into data-retention policies and procedures.
- New systems are included in the quarterly vulnerability scanning process.

SERVICE PROVIDER WRITTEN AGREEMENT (12.8.2)

PCI DSS 3.2.1 further explains that "the extent to which the service provider is responsible for the security of cardholder data will depend on the particular service and the agreement between the provider and assessed entity."

You should obtain a written security acknowledgment from the service provider. In this document, they need to acknowledge their responsibility to protect cardholder data that affects your organization's security.

You need to maintain a list of all PCI requirements your service provider meets and a list of requirements they need to meet.

NEW SERVICE PROVIDER REQUIREMENTS

This section contains the most important new and revised requirements for service providers. Remember, a service provider is an organization that's not a payment brand but is directly involved in the processing, storage, or transmission of cardholder data on behalf of another organization (e.g., managed firewalls, merchant processor).

PENETRATION TESTING REQUIREMENTS (11.3.4.1)

Since February 1, 2018, service providers who use segmentation are required to perform penetration testing (e.g., segmentation checks) on segmentation controls at least every six months and after any changes to segmentation controls/methods.

Validation of your PCI DSS scope should be performed as frequently as possible to ensure your PCI DSS scope remains up to date and aligned with changing business objectives.

Penetration testing should be performed by a qualified internal resource or third party. If applicable, the tester should also have organizational independence (though they aren't required to be a QSA or ASV). The purpose of penetration testing is to test segmentation controls/methods to verify whether they are operational and effective.

If you use segmentation as a service provider, perform penetration tests on segmentation controls at least every six months and after any changes.

Although this requirement only applies to service providers, any organization can request a penetration test whenever they wish to measure their business security.

To find security weaknesses, penetration testers analyze network environments, identify potential vulnerabilities, and try to exploit those vulnerabilities (or coding errors) just like a hacker would.

CRYPTOGRAPHIC ARCHITECTURE (3.5.1)

Service providers need to interview responsible personnel and maintain a documented description of cryptographic architectures, including:

- Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date
- Descriptions of the key usage for each key
- Inventory of any hardware security modules (HSM) and other secure cryptogaphic devices (SCD) used for key management

You must keep pace with evolving threats to your architecture by planning for and documenting updates (e.g., different algorithms/key strengths changes). Maintaining such documentation helps you detect lost or missing keys and key-management devices, as well as helps you identify unauthorized additions to your cryptographic architecture.

TIMELY DETECTION AND REPORTING (10.8, 10.8.1)

Service providers are required to "examine detection and alerting processes and interview personnel to verify that processes are implemented for all security controls, and that failure of a critical security control results in the generation of an alert." Examples of critical security control systems include:

- Firewalls
- IDS/IPS
- FIM
- Anti-virus
- Physical access controls
- Logical access controls
- Audit logging mechanisms
- Segmentation controls (if used)

Service providers must respond to failures of any critical security controls in a timely manner. Processes for responding to security control failures must include:

- Restoring security functions.
- Identifying and documenting the duration (date and time, start to end) of the security failure.
- Identifying and documenting cause(s) of failure (including the root cause) and documenting remediation required to address the root cause.
- Identifying and addressing any security issues that arose during the failure.
- Performing a risk assessment to determine whether further actions are required as a result of the security failure.
- Implementing controls to prevent another failure.
- Resuming monitoring of security controls.

Make sure staff are aware of their responsibilities and that policies and procedures are in place in the event of a security failure. If you are breached, document your organization's actions and responses to the security control failure.

If security failures are not quickly and effectively addressed, attackers may use this time to insert malware, take system control, and steal data from your environment.

ESTABLISH RESPONSIBILITIES FOR PCI AND DATA PROTECTION (12.4.1)

Executive management needs to establish responsibility for the protection of cardholder data and a PCI DSS compliance program, including:

- Overall accountability for maintaining PCI DSS compliance
- Defining a charter for a PCI DSS compliance program and communication to executive management

Smaller organizations should add these roles to an individual's job responsibilities, while larger organizations might need to establish a PCI compliance team (e.g., a compliance team made up of IT, accounting, and management). Whichever is the case, management should give their PCI officer and team power to act and implement necessary changes to become PCI DSS compliant, as well as have monthly–or weekly–meetings with executive management.

QUARTERLY PERSONNEL REVIEWS (12.11, 12.11.1)

Service providers need to perform reviews at least quarterly to confirm personnel are following security policies and operational procedures.

Reviews must cover the following processes:

- Daily log reviews
- Firewall rule-set reviews
- Applying configuration standards to new systems
- Responding to security alerts
- Change management processes

You must also maintain documentation of quarterly review processes, making sure to include:

- Documentation of review results
- Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program

FORENSIC PERSPECTIVE

INTRODUCTION

SecurityMetrics Payment Card Industry Forensic Investigators (PFIs)* thoroughly analyze the point-of-sale (POS) or E-commerce 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 16 consecutive years.

**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.*

WINDOW OF COMPROMISE

HOW LONG ORGANIZATIONS REMAINED VULNERABLE

The window of compromise starts from the date an intruder accesses a business network and ends when the breach is contained by security remediation. Based on data collected by SecurityMetrics Forensic Investigators from 2018 breaches, it took an average of 166 days from the time an organization was vulnerable for an attacker to compromise the system. The average organization was vulnerable for 275 days.

Nearly every organization will experience system attacks from a variety of sources. Due to inherent security weakness in systems or technology, some organizations have systems, environments, software, and website weaknesses that can be exploited by attackers from the day their environment is set up. In other cases, an organization becomes vulnerable because they fail to apply a security patch or make system modifications without properly updating related security protocols.

Once compromised, attackers had access to the sensitive data for an average of 127 days in 2018 investigations. This may be due to aggregation methods employed by data thieves. Attackers have been known to save sensitive data through malware scraping (or other tools), without using or selling the data for months to years.

Using these aggregation methods prevents organizations from identifying malicious account activity until long after the start of the window of compromise, giving the attackers a longer period of time to access vulnerable sensitive data.

2018 SECURITYMETRICS FORENSIC TAKEAWAYS

- The average breached organization was vulnerable for 275 days.
- Cardholder data was captured for an average of 127 days.
- Cardholder data was exfiltrated for an average of 127 days.
- 50% of organizations were breached through remote execution/injection.
- 33% of organizations were breached internally (i.e., employee assisted).
- 17% of organizations were breached through phishing emails.

TERMS TO KNOW

Vulnerable: A state in which a weakness in a system, environment, software, or website could be exploited by an attacker.
Captured: The time that data is being recorded, gathered, and/or stored from an unauthorized source.
Exfiltrated: The unauthorized transfer of data from a system.

2019 FORENSIC PREDICTIONS

PREDICTION 1

Passwords may not be the security you're looking for. We will start to see next year—and more so in the coming years—that passwords will no longer be considered an element of security. There is current technology that can search and break password hashes at a rate of 600 billion attempts per second. This means that attackers could span every possible combination of keys, in most languages, in just a few days. As developers put more steam behind this tool, the time and resources needed to break passwords will greatly reduce, regardless of password complexity level.

PREDICTION 2

Biometric data will be compromised. Information like fingerprints and other biometric scans needs to be stored somewhere. But if data can be stored, it can also be stolen. Just as there are large repositories of stolen username/password combinations available for sale on the dark web, stolen biometric data will follow as well.

PREDICTION 3

A major cloud storage provider will be seriously breached. With so many businesses and individuals uploading massive amounts of data to the cloud, it's only a matter of time before hackers figure out a way to get to it.

PREDICTION 4

Foreign nation-states will increase recruitment of corporate insiders to steal insider secrets.

PREDICTION 5

Large-scale social-media-based hacks will lead to massive data losses. For example, many individuals play games through their social media accounts. Related to some of these games are offers for the user to receive "unlimited coins" and "unlimited lives" via a third-party site. In exchange for these coins and lives, users are asked to download apps from the provider. Often, the provider will state that the purpose of requiring the app download is that it "proves you're not a robot" or it "helps keep the offerings free."

One of our forensic investigators installed some of these games and app downloads into a sandbox environment and found that they were actually VPNs–giving the providers a backdoor into the user's device. With kids and adults regularly downloading these games and apps to devices, a social media/game hack is going to lead to a massive data breach.

PREDICTION 6

Artificial intelligence (AI) will be on your side and against you. We will likely soon start to see security tools with artificial intelligence that can detect and adapt to data breaches. But we will also likely see AI on the attackers' side–with malware that can self-move, self-manipulate, and self-hide in response to what it sees a user do. AI will start to show up with increasing frequency, and it's going to make the future of data security very interesting.

PCI DSS REQUIREMENTS

REQUIREMENT 1:

PROTECT YOUR SYSTEM WITH FIREWALLS

Network firewalls are vital for your security. A firewall's purpose is to filter potentially harmful Internet traffic to protect valuable sensitive data. Simply installing a firewall on your organization's network perimeter doesn't make you secure.

HARDWARE FIREWALLS

A hardware firewall–or perimeter firewall–is typically installed at the perimeter of an organization's network to protect the internal networks from the Internet. Hardware firewalls are also used inside an environment to create isolated network segments. Higher security internal network segments would be created to limit access to sensitive data from networks that don't need that access.

In summary, a properly configured hardware firewall protects environments from the outside world. For example, if attackers try to access your network from the outside, your hardware firewall would act as the first line of defense and should block them.

HARDWARE FIREWALL PROS	HARDWARE FIREWALL CONS
Most robust security option	Rules need to be carefully documented
Protects an entire network	Difficult to configure properly
Can segment internal parts of a network	Needs to be maintained and reviewed regularly

SOFTWARE FIREWALLS

You also need a firewall between systems that store sensitive data and other systems on your network. Typically, this is a second hardware firewall installed inside your corporate network to create a secure zone to further protect sensitive data.

Many personal computers come with pre-installed software firewalls. This feature should be enabled and configured for any laptop computers that commonly connect to sensitive data networks. For example, if a sales manager accidentally clicks on a phishing email scam, their computer's software firewall should stop the malware from propagating through the corporate network.

SOFTWARE FIREWALL PROS	SOFTWARE FIREWALL CONS
Protects mobile workers when outside the corporate network	Should not replace hardware firewalls for network segmentation
Easier to maintain and control	Doesn't protect an entire network
Inexpensive	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 filter potentially harmful Internet traffic and other untrusted networks to protect valuable confidential data. In e-commerce applications, a firewall should be used to limit traffic to only 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 into and out of these zones, and more easily protect payment data.

In a recent 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 essentially negated the whole firewall, leaving the entire network exposed. It was through this vulnerability that the attacker accessed their network and stole sensitive data.

FIVE BASIC 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, justify need for rules, consider both inbound and outbound traffic, etc.).

2. **TRUST BUT VERIFY:** After implementing firewall rules/ settings, test the firewall appropriately externally and internally to confirm settings are correct (pen test, scans, etc.).

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 to just what is needed, this limits hackers' paths for exfiltrating data.

4. **PERSONAL FIREWALLS:** Configure personal firewalls on mobile computing platforms to limit attack surfaces and minimize propagation of malware when on unsecured networks.

5. **MANAGEMENT:** Only manage the firewall itself from within your network, disable external management services unless it's part of a secure managed firewall infrastructure.

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 2018's 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, work station) to the CDE or other sensitive systems.

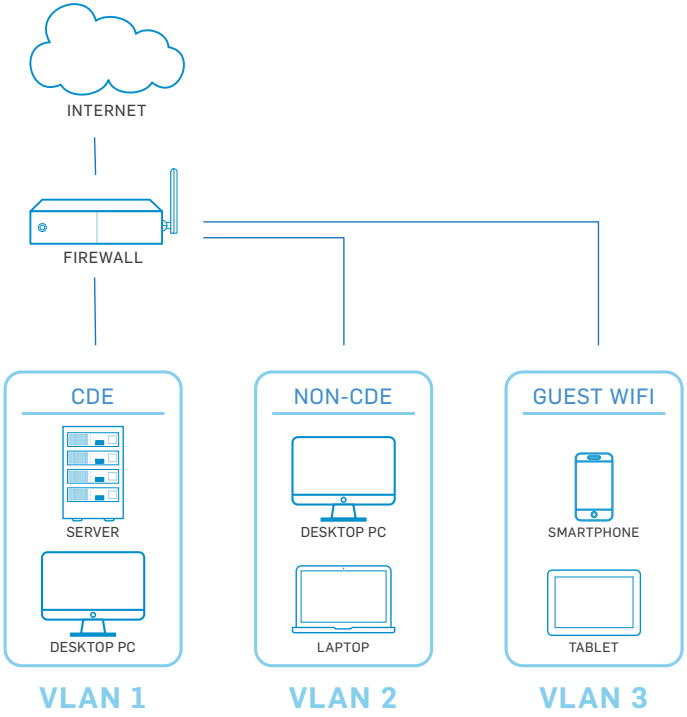
Firewalls can be used to segment an organization's network. When businesses create a secure payment zone–firewalled off from the rest of the day-to-day business traffic–they can better ensure their CDE only communicates with known and trusted sources. This limits the size of the CDE and potentially lowers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

For example, you install and configure a multi-interface firewall at the edge of your network. From there, you 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 other zones, this is proper network segmentation.

Segmentation is not necessarily required in order to be compliant with PCI DSS 3.2.1. However, if you're looking for one of the easiest ways to reduce cost, effort, and time getting in-scope systems compliant, 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 all your segmentation work by performing regular 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 or at least every six months.

TIPS FROM AN AUDITOR

REQUIREMENT 1: ESTABLISH THOROUGH FIREWALL ARCHITECTURE

Large environments typically have firewalls in place, at least at the network's perimeter. 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.

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.

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 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 line, if you or any third parties remotely support your environment, limit that inbound access to specific sources and protocols.

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

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. This will help you pick out the important data that requires your action.

For requirement 1, remember the following:

- Start with a "block everything" mentality, then work backwards.
- Pay attention to what logs tell you.
- Review firewall configurations frequently and adjust as necessary.

GEORGE MATEAKI
QSA | PA-QSA | CISSP | CISM | CISA

REQUIREMENT 1 IT CHECKLIST

FIREWALL IMPLEMENTATION AND REVIEW

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- [ ] Firewall(s)
- [ ] "Deny All" rule for all other inbound and outbound traffic (1.2.1.b)
- [ ] Stateful inspection/dynamic packet filtering (1.3.5)
- [ ] Documented business justification for each port or protocol allowed through the firewall (1.1.6a)

THINGS YOU WILL NEED TO DO:

- [ ] Limit traffic into the CDE to that which is necessary. (1.2.1.a)
- [ ] Position firewall(s) to prohibit direct inbound and outbound traffic from the CDE. (1.3)
- [ ] Create secure zone(s) for any card data storage, which must be separate from DMZ. (1.3.6)
- [ ] Explicitly authorize outbound connections from the CDE. (1.3.4)
- [ ] Document all firewall policies and procedures. (1.2.1.a, 1.2.1.b, 1.2.3, 1.3, 1.3.3, 1.3.5, 1.3.6)

THINGS YOU MAY NEED TO DO:

- [ ] Install a firewall between wireless networks and the CDE (wireless only). (1.2.3)

REQUIREMENT 2:

USE ADEQUATE CONFIGURATION STANDARDS

DEFAULT PASSWORD WEAKNESSES

Out-of-the-box devices, such as routers or POS systems, come with factory settings like default usernames and passwords. Defaults make device installation and support easier, but also mean every model originates with the same username and password. Default passwords are easy to guess, especially since most 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; however, 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 both numbers and letters.

Passwords that fall short of these criteria can usually be broken using a password-cracking tool.

SYSTEM HARDENING

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

According to requirement 2.2, you must "address all known security vulnerabilities and [be] consistent with industry-accepted system hardening standards."

Here are 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 are capable of scanning and reporting on hardware and software used in a network and also detecting 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.

TIPS FROM AN AUDITOR

REQUIREMENT 2: SYSTEM CONFIGURATION

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 systems 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 opens you up to additional risk and possible vulnerability.

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.

GEORGE MATEAKI
QSA | PA-QSA | CISSP | CISM | CISA

REQUIREMENT 2 IT CHECKLIST

CONFIGURATION STANDARDS

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- [ ] A secure way to access and manage systems in your environment (2.3)
- [ ] An inventory of all hardware and software used in your CDE
- [ ] Documented configuration standards for all types of systems in your CDE

THINGS YOU WILL NEED TO DO:

- [ ] Assign system administrator and knowledgeable personnel the responsibility of configuring system components. (2.2.4)
- [ ] Implement a system hardening guide that covers all system components of your CDE. (2.2.a)
- [ ] 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. (2.2.2, 2.2.3, 2.2.5)
- [ ] 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). (2.1.a, 2.1.b, 2.1.1.b, 2.1.1.c, 2.1.1.d, 2.1.1.e)
- [ ] 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. (2.4, 2.5)

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. (2.1.1.d, 2.3)
- [ ] If wireless Internet is enabled in your CDE, change wireless default settings including encryption keys, passwords, and SNMP community strings. (2.1.1)
- [ ] Enable only one primary function per server (e.g., logging server, web server, DNS). (2.2.1)

REQUIREMENT 3:

SECURE CARDHOLDER 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 don't know that they store unencrypted primary account numbers (PAN).

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.

2019 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 2 billion unencrypted PANs on business networks. In 2018, users scanned over 3,600 computers and 7,000,000 GBs. Here are some key statistics:

- 85% of PANscan® users discovered unencrypted PAN data
- 5% stored track data (i.e., data inside magnetic stripe)
- Over 330 million PANs were found

In the latest SecurityMetrics study, 85% of PANscan® users found unencrypted PAN data on their network.

KNOW WHERE ALL CARDHOLDER DATA RESIDES

An essential part of eliminating stored card data is using a valid card data discovery tool and methodology. 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 CHD flow diagram is a graphical representation of how card data moves through an organization. As you define your environment, it's important to ask all organizations and departments if they receive cardholder information, and then define how their answers may change CHD flows.

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? Real time or end of day?
- How is data authorized and returned by the processor?
- Is card data backed up on my system? Are backups encrypted? Is my backup server at a different data location?
- Where might card data be going or moved in processes not part of authorization and settlement?

In addition, you should regularly run a cardholder data discovery tool. These tools help identify the location of unencrypted PAN so you can securely delete or encrypt it. They also help identify which processes or flows might need to be fixed.

Once you identify new processes, you can begin to determine how to either fix the process or add it into your normal environment flow.

	DATA ELEMENT	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

TIPS FROM AN AUDITOR

REQUIREMENT 3: PROTECT CARDHOLDER DATA

Some of the biggest data issues organizations face are: having a data retention policy, understanding their policy, and following their policy.

IT security should work with the legal and executive teams to decide what data the company holds onto, why they need it, and the length of time it's held. However, this communication often doesn't happen. Security staff will often draft data security policies to meet PCI DSS compliance, but if it isn't adopted and enforced from the executives down, company processes will never change.

Policy enforcement must include requirements to encrypt data once it is received, time frames to keep data, and a documented procedure to delete unnecessary payment card data that does not meet policy specifications.

Next, it's imperative to understand what data you actually have. Map out all the flows to understand where data moves in your organization. For example, you may not know that the accounting department captures card data from a database and stores it in spreadsheets or that cardholder data is being saved in log files.

The best practice to find unencrypted data is through a card data discovery tool.

Once all card data is found, make sure you consult your security policies and PCI DSS to determine what you are allowed to keep. For example, PCI DSS prohibits storage of track data.

Make sure to limit exposure to systems that handle card data by keeping all networks segmented and limiting the amount of card data stored.

GEORGE MATEAKI
QSA | PA-QSA | CISSP | CISM | CISA

REQUIREMENT 3 IT CHECKLIST

SECURING CARDHOLDER DATA

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- [ ] A documented data retention policy
- [ ] A data flow diagram

THINGS YOU WILL NEED TO DO:

- [ ] Have employees acknowledge their training and understanding of the policy. (3.1, 3.6.8, 3.7)
- [ ] Eliminate storage of sensitive authentication data after card authorization. (3.2.d, 3.2.1, 3.2.2, 3.2.3)
- [ ] Mask out PAN on customer receipts. (3.3)
- [ ] Understand guidelines for handling and storing cardholder data.

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. (3.4)
- [ ] 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 hardcopy of stored details. (3.4.1, 3.5, 3.5.2, 3.5.3, 3.5.4, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7)

REQUIREMENT 4:

SECURE DATA OVER OPEN AND PUBLIC NETWORKS

For requirement 4, you need to identify where you send cardholder data. The following are common places 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, if your organization has existing implementations of SSL and early TLS not necessary for regular business operations, immediately remove or discontinue all instances. The only acceptable use of these outdated protocols is if your POS/POI hardware currently in use does not support later versions of secure TLS.

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

Examples of applications that may 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 those insecure protocols. Check with your merchant bank or POS/POI supplier if you have questions on that.

Service providers that support older POS/POI terminals that still use the insecure SSL/TLS protocols still should have a Risk Mitigation and Migration Plan in place. According to the PCI Council, this document will "detail [your] plans for migrating to a secure protocol, and also describe controls [you have] in place to reduce the risk associated with SSL/early TLS until the migration is complete."

TIPS FROM AN AUDITOR

REQUIREMENT 4: SENDING DATA OVER OPEN AND PUBLIC NETWORKS

To begin with, you need to know exactly how and where you are sending cardholder information so that you can know what needs to be encrypted during transmission.

It's important to have a good understanding of technologies (e.g., SSL, TLS) and where your organization stands regarding your security processes. If you've already eliminated outdated processes, great. If not, the only accepted use(s) of these older protocols are for POS/POI hardware and service providers that support them.

You must transition away from these older technologies as quickly as possible to be secure and compliant to the PCI DSS. You might be worried about losing business with customers using older browsers (e.g., SSL, early TLS). In reality, there will likely be a limited negative impact on customers, if at all.

If I were you, I would eliminate using these outdated technologies because it's better to be safe than to risk a security breach.

GEORGE MATEAKI
QSA | PA-QSA | CISSP | CISM | CISA

REQUIREMENT 4 IT CHECKLIST
TRANSMITTING CARDHOLDER DATA

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- [ ] An in-house policy to ensure you do not send unprotected PANs via end-user messaging technologies (4.2.b)

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. (Appendix A2)
- [ ] 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. (Appendix A2.1)
- [ ] 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. (4.1, 4.1.1)
- [ ] 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. (4.1)
- [ ] Review and implement documented encryption standard best practices (4.1.1)
- [ ] Review and implement policies and procedures for sending and receiving credit card data. (4.2.b)
- [ ] Examine system configuration and adjust encryption configuration as needed. (4.1, 4.1.1)

THINGS YOU MAY NEED TO DO:

- [ ] Make sure TLS is enabled whenever cardholder data is transmitted or received through web-based services. (4.1.a, 4.1.e)
- [ ] Check wireless network encryption standards. (4.1.1)
- [ ] Examine keys and certificates. (4.1.b)
- [ ] If you are a service provider supporting older POS/POI terminals, review your Risk Mitigation and Migration Plan for environments that still need to use SSL and early TLS. (Appendix A2.2)
- [ ] Prohibit the use of WEP–an insecure wireless encryption standard. (4.1.1)

REQUIREMENT 5:

PROTECT SYSTEMS WITH ANTI-VIRUS

REGULARLY UPDATE YOUR ANTI-VIRUS

Anti-virus software needs to be installed on all systems commonly affected by malware, regardless of its location. Make sure anti-virus or anti-malware 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-virus scanning. If your vendor doesn't handle your anti-virus, 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-virus threat feeds, merchants can identify emerging malware and attacks on systems. They should then configure systems to alert and report on 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 hackers to successfully attack your systems and steal valuable data. As part of your vulnerability management strategy, make sure to include updated anti-virus software.

TIPS FROM AN AUDITOR

REQUIREMENT 5: IMPLEMENT AND UPDATE YOUR ANTI-VIRUS

Anti-virus software offers an additional layer of security to any system within a network. System administrators have the responsibility of making sure their anti-virus software, including the signatures, are up to date.

This applies to either a master anti-virus server client-based configuration or single server/workstation installations. Additionally, PCI DSS requires anti-virus scanning to occur on a regular basis.

PCI DSS requires anti-virus 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-virus software be installed for any web-facing Linux server. Malicious coders still target Linux systems as well as Windows. The risk is too great not to run anti-virus software on web-facing Linux systems.

When system administrators understand that anti-virus software adds another line of defense for their environment, they have an advantage when it comes to securing the sensitive data it contains.

MICHAEL OHRAN
QSA | PA-QSA | CISSP

REQUIREMENT 5 IT CHECKLIST

ANTI-VIRUS UPDATES

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO DO:

- [ ] Deploy anti-virus software on commonly affected systems (5.1, 5.2)
- [ ] Protect all systems against malware and regularly update anti-virus software or programs. (5.1, 5.2.b)
- [ ] Ensure anti-virus programs can detect, remove, and protect against all known types of malicious software. (5.1.1)
- [ ] Maintain and evaluate audit logs with IT staff. (5.2.c)
- [ ] Set anti-virus program to scan automatically. (5.2.b)
- [ ] Make sure anti-virus program is updated automatically (with definitions kept current). (5.2.a, 5.2.b)
- [ ] Ensure anti-virus program cannot be disabled or altered by users (i.e., admin access only). (5.3)
- [ ] Document and review malware procedures; review with necessary staff. (5.4)
- [ ] Examine system configurations and periodically evaluate malware threats to system. (5.1.2)

REQUIREMENT 6:

UPDATE YOUR SYSTEMS

REGULARLY UPDATE AND PATCH SYSTEM(S)

Application developers will never be perfect, which is why updates to patch security holes are frequently released. Once a cyber criminal knows they can get through one of these security holes, they pass that knowledge on to other criminals. They could then exploit this weakness until the patch has been updated.

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 XP, Windows Server 2003).

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 6.2 states that organizations must "install critical patches within a month of release" to maintain compliance. 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 potential 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., e-commerce 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 6.6 requires public-facing web applications to regularly monitor, detect, and prevent web-based attacks, such as implementing 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 cyber security alert if it detects attack patterns.

WEB APPLICATION FIREWALL PROS	WEB APPLICATION FIREWALL CONS
Immediate response to web application security flaws	Requires more effort to set up
Protection for third-party modules used in web applications	Possibly break critical business functions (if not careful)
Deployed as reverse proxies	May require some network re-configurations

TIPS FROM AN AUDITOR

REQUIREMENT 6: SYSTEM UPDATING AND SOFTWARE DEVELOPMENT

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 postures.

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 sub-section 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 environment 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. 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 standard 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 recently 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.

MICHAEL OHRAN
QSA | PA-QSA | CISSP

REQUIREMENT 6 IT CHECKLIST

SOFTWARE UPDATES

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- ☐ Vendor supported programs, operating systems, and devices (6.2)
- ☐ 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. (6.1, 6.5.6)
- ☐ Install all vendor-supplied security patches on all system components. (6.2.a)
- ☐ Ensure all security updates are installed within one month of release. (6.2.b)

THINGS YOU MAY NEED TO DO:

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

REQUIREMENT 7:

RESTRICT ACCESS

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 3.2.1 requires a defined and up-to-date list of the roles with access to the cardholder data environment. 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 a maintenance professional. You need to define and document what kind of user permissions they have.

TIPS FROM AN AUDITOR

REQUIREMENT 7: RESTRICT ACCESS

This requirement is one of the oldest and most basic parts of the PCI DSS.

Things haven't really changed for this requirement. There's no new trend or solution. But not all organizations have accurately complied 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.

MICHAEL OHRAN
QSA | PA-QSA | CISSP

REQUIREMENT 7 IT CHECKLIST
ESTABLISH ACCESS CONTROL

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- ☐ Written policy detailing access controls for systems in the CDE (7.1, 7.3)

REQUIRED FEATURES:

- ☐ Documented access control policies based on job classification and function (7.1, 7.1.1, 7.1.2, 7.1.3)
- ☐ Roles and privilege levels defined (7.1, 7.1.1)
- ☐ "Deny all" rule in place for access control systems (7.2.3)

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. (7.1, 7.1.4)
- ☐ Document policies in place with each employees' role/access and train employees on their specific access level. (7.1, 7.3)

THINGS YOU MAY NEED TO DO:

- ☐ Implement access controls on any systems where cardholder data is stored and handled. (7.2.1)
- ☐ Configure access controls to only allow authorized parties and deny all others without prior approval or access. (7.2.2, 7.2.3)

REQUIREMENT 8:

USE UNIQUE ID CREDENTIALS

WEAK PASSWORDS AND USERNAMES

If a username and password don't meet the recommended security standards for length, uniqueness, and complexity, it will be that much easier for an attacker to gain access to your environment. An attacker may try a brute-force attack against a system by leveraging a rainbow table of common passwords in an attempt to escalate privileges or by using an automated tool to try and guess the password of a user account to gain system access.

PCI DSS requires passwords to be changed every 90 days and have at least seven characters of both numbers and letters. Passwords that fall short of this criteria can easily be broken using a password-cracking tool. In practice, the longer the password and the more character formats allowed, the more difficult it will be for an attacker to crack a password. The risk is that when a password gets to be too hard to remember that it is often written down and placed where in an easy to access location. Update your company password policy so that increasing the complexity doesn't undermine security objectives.

Disabling 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), businesses should have unique usernames. A company is much more secure if an attacker has to first guess the username before cracking its corresponding password.

PCI requires an account lock be set to 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 a hacker has to go through, the more likely it is they will move on to an easier target.

IMPLEMENT MULTI-FACTOR AUTHENTICATION

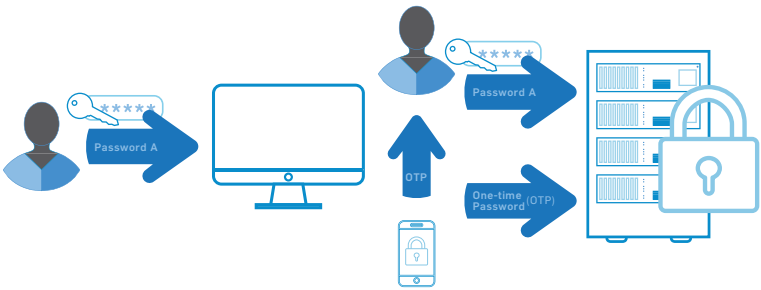
System security should not be based solely on the complexity of a single password. No password should be considered uncrackable. That's why multi-factor authentication (MFA) is the most effective solution to secure remote access and is a requirement under the PCI DSS.

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

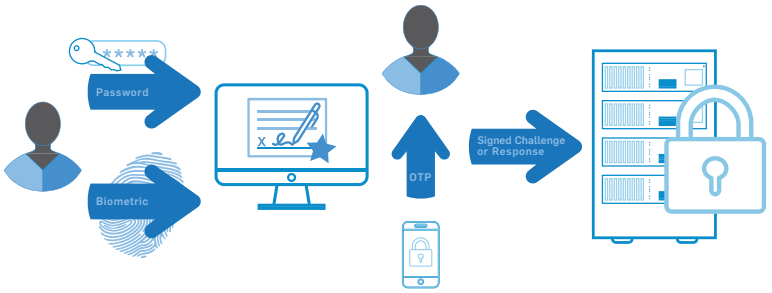
- Something you *know* (e.g., a username and password, PIN number)
- Something you *have* (e.g., hardware token, smartcard)
- Something you *are* (e.g., a fingerprint, ocular scan, voiceprint)

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

- 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.



- 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.



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."

If a remote access application configuration only requires a username and password, the application has been configured insecurely.

TIPS FROM AN AUDITOR

REQUIREMENT 8: USE UNIQUE ID CREDENTIALS

Requirement 8 is all about having unique ID information. For example, you must have your own unique ID credentials and account on your portable devices, with strong password cryptography.

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

As a system administrator, it's a best practice 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.

All non-console administrative access to in-scope systems requires multi-factor authentication.

Security professionals recognize that passwords are no longer sufficient to secure data. Passwords are still required, but simply not secure enough. You must set strong, long passwords. To meet PCI requirements, a password must contain at least seven characters and be complex, with both alphabetic and numeric characters.

An easy way to remember complex passwords is by using passphrases. Passphrases are groups of words with spaces in between (e.g., "We Never Drove Toward Vancouver?"). 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. Some password managers can even work across multiple devices through the use of a cloud-based service.

You really need different passwords for different services, so that if one service gets compromised, it doesn't bleed into other sites' passwords.

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.

MICHAEL MAUGHAN
QSA | CISA | CISSP

REQUIREMENT 8 IT CHECKLIST

ID CREDENTIALS

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- ☐ Multi-factor authentication for all remote access (8.3)

THINGS YOU WILL NEED TO DO:

- ☐ Monitor all remote access accounts used by vendors, business partners, IT support personnel, etc. when the account is in use. (8.1.5.b)
- ☐ Disable all remote access accounts when not in use. (8.1.5.a)
- ☐ Enable accounts used for remote access only when they are needed. (8.1.5.a)
- ☐ Implement a multi-factor authentication solution for all remote access sessions.
- ☐ Configure multi-factor authentication with at least two of the following methods (8.3):
  - ☐ 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)

REQUIREMENT 9:

ENSURE PHYSICAL SECURITY

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, when your staff is too busy with assignments to notice someone walking out of the office with a server, laptop, or other mobile device.

Control 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 who have services that require repeat billing keep physical copies of credit card information in easily accessible areas for convenience. While this collection of files may make life easier, it puts valuable cardholder data at risk of being stolen 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 implemented, especially when individuals are terminated or their job role and responsibilities change.

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

The majority of physical data thefts take only minutes to plan and execute.

In addition, make sure all workstations have an automated timeout/logout on computers and devices (e.g., a password-protected screensaver pops up on a computer after a set amount of time). This makes it more difficult for unauthorized users to access data from these workstations when employees aren't there.

KEEP TRACK OF POS TERMINALS

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

1. **Maintain an up-to-date list of all devices (9.9.1)** including physical location, serial numbers, make, and model.
2. **Periodically inspect devices (9.9.2).** 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 (9.9.3)** 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.

TRAIN EMPLOYEES EARLY AND OFTEN

While you may understand how to protect customer card information, your employees may not. That's why regular security trainings are so important.

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 further identify them and verify their presence?

Train your employees to question everything. 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.

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 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.

TIPS FROM AN AUDITOR

REQUIREMENT 9: IMPROVE YOUR PHYSICAL SECURITY

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 basic 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).

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 areas and limit access only to individuals with approved access. 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.

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 and screws.

MICHAEL MAUGHAN
QSA | CISA | CISSP

REQUIREMENT 9 IT CHECKLIST
IMPROVING PHYSICAL SECURITY

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

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

THINGS YOU WILL NEED TO DO:

- [ ] Restrict access to any publicly accessible network jacks. (9.1.2)
- [ ] Keep physical media secure and maintain strict control over any media being moved within the facility and outside of it. (9.5, 9.5.1, 9.6.a)
- [ ] 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. (9.6.1, 9.6.3, 9.7)
- [ ] Use a secure courier when sending media through the mail so the location of the media can be tracked. (9.6.2)
- [ ] 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. (9.8, 9.8.1)
- [ ] 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. (9.9.2, 9.9.3)

THINGS YOU MAY NEED TO HAVE:

- [ ] 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.

REQUIREMENT 10:

IMPLEMENT LOGGING AND LOG MONITORING

SYSTEM LOGS AND ALERTING

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

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. They're your lookouts and can provide the warning data that could alert you to a data breach. 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

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. Log monitoring software takes care of this issue by using rules to automate log review and only alert on events that might be real problems. Often this is done using real-time reporting software that sends you alerts 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 take time to correctly configure your alerting rules at the beginning.

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

To take advantage of log management, look at your security strategy 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 an employee you trust to review logs daily.
- Set up a team to review suspicious alerts.
- 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.
- Confirm everything is being appropriately logged.

Regular 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, it will also help defend against internal and external threats.

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

TIPS FROM AN AUDITOR

REQUIREMENT 10: AUDIT LOGS AND LOG MONITORING

Given the large amount of log data generated by systems, it's virtually impossible to manually analyze logs beyond one or two systems.

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 smaller companies now realize system monitoring can help identify attacks.

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.

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

PCI DSS 3.2.1 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 also identify risks created by the failure, identify root causes, document lessons learned, and implement any necessary changes to prevent failures from happening again.

MICHAEL MAUGHAN
QSA | CISA | CISSP

REQUIREMENT 10 IT CHECKLIST
LOGGING AND LOG MANAGEMENT

*Assigned to:*_____

*Assignment date:*_____

*Completion 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 root or administrative privileges (10.2.2)
  - ☐ Failed log-in attempts (10.2.4)
  - ☐ Changes to accounts–including elevation of privileges, account additions, and account deletions (10.2.5)
  - ☐ 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 (10.3.1-10.3.6)

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. (10.6.1.b, 10.6.2.b)
- ☐ Have a process in place to respond to anomalies and exceptions. (10.6.3.b)
- ☐ Keep all audit log records for at least one year and keep the last three months' logs readily available for analysis. (10.7.b, 10.7.c)

REQUIREMENT 11:

CONDUCT VULNERABILITY SCANS AND PENETRATION TESTS

UNDERSTAND YOUR ENVIRONMENT

A business's IT environment influences the kind of attacks to which they're susceptible; therefore, every security plan should be tailored to each individual network environment.

Defects in web browsers, email clients, POS software, operating systems, and server interfaces can allow attackers to gain access to an environment. Installing security updates and patches for systems in the cardholder or sensitive data environments can help correct many of the newly-found defects and vulnerabilities before attackers have the opportunity to leverage them.

In the case of custom in-house applications, code testing and independent internal penetration testing can expose many of the weaknesses commonly found in application code (especially home-grown varieties). These types of tests are the best line of defense in identifying weaknesses before deployment.

VULNERABILITY SCANNING BASICS

A vulnerability scan is an automated, high-level test that looks for and reports potential vulnerabilities. All external IPs and domains exposed in the CDE are required to be scanned by a PCI Approved Scanning Vendor (ASV) at least quarterly.

PCI DSS requires two independent methods of PCI scanning: internal and external scanning. An *external vulnerability scan* is performed outside of your network; it identifies known weaknesses in network structures. An internal vulnerability scan is performed within your network, and it looks at other hosts on the same network to identify internal vulnerabilities.

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 are locked.

Vulnerability scanning identifies potential harmful vulnerabilities, so you can remediate processes to ensure network security.

Typically, vulnerability scans will generate an extensive report of discovered vulnerabilities and references for further research on these vulnerabilities. Some reports even offer further directions for how to fix the problems.

Despite what many businesses believe, scanning is not enough. You can't just scan and sit on the report. Act quickly on any vulnerabilities to ensure security holes are plugged, and then re-scan to validate that the vulnerabilities have been successfully addressed.

VULNERABILITY SCANNING PROS	VULNERABILITY SCANNING CONS
Quick, high-level look at possible vulnerabilities	False positives
Very affordable compared to penetration testing	Businesses must manually check each vulnerability before testing again
Automatic (can be automated to run weekly, monthly, quarterly)	Does not confirm a vulnerability is possible to exploit

RUN EXTERNAL VULNERABILITY SCANS

For many organizations, external scans must be performed by a PCI ASV to validate PCI compliance.

An ASV is required to go through a rigorous yearly recertification process, during which each ASV runs their PCI scanning tool on PCI Council-approved sites planted with vulnerabilities to test which vulnerabilities the tool finds and misses.

Just because an ASV runs your external vulnerability scan, doesn't mean your organization is secure. After receiving your scan report, you're responsible for fixing discovered vulnerabilities and then re-scanning your environment until vulnerabilities have been properly addressed.

RUN INTERNAL VULNERABILITY SCANS

People often assume that if an ASV handles their PCI scans, it means they're compliant. However, if your ASV currently performs your external quarterly scans, understand they're not likely handling your internal quarterly vulnerability scanning.

Your ASV may have set up an internal vulnerability scanning tool or appliance, but chances are that they're not handling or monitoring your internal vulnerability scanning requirements. Make sure that your internal vulnerability scans are routinely performed.

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 service provider.
- Download an open source internal 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.

Typically, if you purchase a vulnerability scanning tool or appliance, IT support service is included. But if you download scanning tools, take time to research and implement configuration best practices.

Remember, when it comes to vulnerability scanning, your organization is responsible for the configuration, actual scanning, alert analysis, and vulnerability remediation.

PENETRATION TESTING BASICS

Similar to a hacker, penetration testers analyze network environments, identify potential vulnerabilities, and try to exploit those vulnerabilities (or coding errors). In simple terms, penetration testers attempt to break into your company's network to find security holes and let you know about discovered vulnerabilities.

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

Depending on your SAQ, PCI DSS requirement 11.3 may require an internal and external penetration test. But penetration testing isn't limited to the PCI DSS. Anyone can request a penetration test to measure their business's security.

The time it takes to conduct a penetration test varies based on network size, network 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 several weeks.

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

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

PENETRATION TESTING PROS	PENETRATION TESTING CONS
Live, manual tests mean more accurate and thorough results	Time (1 day to 3 weeks)
Rules out false positives	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.

Commonly identified security issues include:

- Misconfigured software, firewalls, and operating systems
- Outdated software and operating systems
- Insecure protocols

SEGMENTATION CHECK

The objective of a segmentation check is to identify whether there is access into a secure network because of a misconfigured firewall. Basically, segmentation checks confirm if network segmentation was set up properly.

For service providers that use segmentation, you're required to conduct penetration tests on segmentation controls every six months and after any significant change to segmentation controls/methods.

Commonly identified security issues include:

- TCP access is allowed where it should not be
- 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 publishing of the software.

Commonly identified security issues include:

- Injection vulnerabilities (e.g., SQL injection, cross-site scripting, 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)
- Improper error handling

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 security issues include:

- Insecure wireless encryption standards
- Weak encryption passphrase
- Unsupported wireless technology
- Rogue and open access points

SOCIAL ENGINEERING

The objective of a social engineering assessment is to identify employees that do not properly authenticate individuals, follow processes, or validate potentially dangerous technologies. Any of these methods could allow an attacker to take advantage of the employee and trick them into doing something they shouldn't.

Commonly identified security issues include:

- Employee(s) clicked on malicious emails
- Employee(s) allowed unauthorized individuals onto the premises
- Employee(s) connected a randomly discarded or discovered USB to their workstation

VULNERABILITY SCANNING VS. PENETRATION TESTING

Some mistakenly believe vulnerability scans are the same as professional penetration tests.

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, while a *penetration tester* digs deeper to identify the root cause of the vulnerability that allows access to secure systems or stored sensitive data.

Vulnerability scans and penetration tests work together to encourage optimal network security.

Vulnerability scans are great weekly, monthly, or quarterly insight into your network security, while penetration tests are a more thorough way to examine your security.

TIPS FROM AN AUDITOR

REQUIREMENT 11: PENETRATION TESTING

Whenever large infrastructure changes occur, PCI DSS requires a formal penetration test to see if the changes added any new vulnerabilities.

Even though the necessity for an annual penetration test is apparent, organizations often claim that they made no significant infrastructure changes because the cost and time of a full-blown penetration test can seem overwhelming.

My advice is this: first establish what your organization considers a major change. What might be a major change to a smaller organization is only a minor change in a large environment. For either size organization, if you bring in new hardware or start accepting payments in a different way, this constitutes a major change.

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

The next step is to establish an assessment policy. Some organizations designate a department separate from the infrastructure team to conduct self-assessments. Others hire penetration testers to conduct these types of assessments.

GEORGE MATEAKI
QSA | PA-QSA | CISSP | CISM | CISA

REQUIREMENT 11 IT CHECKLIST

VULNERABILITY SCANNING & PENETRATION TESTING

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- ☐ A process for detecting and identifying wireless access points on a quarterly basis. The method should be able to identify all of the following wireless access points:
  - ☐ WLAN cards inserted into system components
  - ☐ Mobile devices used to create wireless access points (by USB or other means
  - ☐ Wireless devices attached to a network port or device (11.1.a, 11.1.b, 11.1.c)
- ☐ An inventory of authorized wireless access points with listed business justifications (11.1.1)
- ☐ A change-detection mechanism installed within the CDE to detect unauthorized modifications to critical system files, configuration files, or content files (11.5.a)

THINGS YOU WILL NEED TO DO:

- ☐ Run quarterly internal vulnerability scans using a qualified internal resource or external third party (in either case, organizational independence must exist), and then re-scan all scans until high-risk (as defined in requirement 6.1) vulnerabilities are resolved. (11.2.1)

- [ ] Run quarterly external vulnerability scans (through an ASV) and then re-scan until all scans obtain a passing status (i.e., no vulnerability scores over 4.0). (11.2.2)
- [ ] Run internal and external scans, using a qualified resource, after any significant change to the network, and re-scan until resolved:
  - [ ] For *external scans*: No vulnerabilities scoring 4.0 or higher exist (11.2.2)
  - [ ] For *internal scans*: All high-risk vulnerabilities are resolved (11.2.3)
- [ ] Configure your change-detection mechanism to alert personnel to unauthorized modification of critical system files, configuration files, or content files; configure the tools to perform critical file comparisons at least weekly. (11.5.b)
- [ ] Have a process in place to respond to alerts generated by your change-detection mechanism. (11.5.1)

THINGS YOU MAY NEED TO DO:

- [ ] If wireless scanning is used to identify wireless access points, scans must be run at least quarterly. (11.1.c)
- [ ] If automated monitoring is used, monitoring should generate alerts to notify personnel. (11.1.d)
- [ ] Create a plan of action in your business's incident response plan for responding to the detection of unauthorized wireless access points, and take action if unauthorized wireless access points are found. (11.1.2)
- [ ] If network segmentation exists, penetration testing procedures must confirm that segmentation is operational and isolates all out-of-scope systems from systems in your CDE. (11.3.4.a)

REQUIREMENT 12:

START DOCUMENTATION AND RISK ASSESSMENTS

REGULARLY DOCUMENT BUSINESS PRACTICES

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

Documentation may also help 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.

If you are a service provider, your executive management is required to implement a PCI DSS Charter. This Charter must establish responsibility for the protection of cardholder data and create 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.

To fulfill requirement 12.8.5, you must have a list of all third-party service providers you use, the PCI requirements these service providers handle, and the PCI requirements you are required to meet.

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

- Employee manuals
- Policies and procedures
- Third-party vendor agreements
- Incident response plans

Regularly-updated documentation of all security measures and actions is vital for PCI compliance.

ESTABLISH A RISK ASSESSMENT PROCESS

Requirement 12.2 requires all entities to perform an annual risk assessment that identifies critical assets, threats, vulnerabilities, and risks. This requirement 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 vulnerability 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 network. This will help provide direction on what vulnerabilities you should address first. Mitigating vulnerabilities can decrease the time an attacker can access and negatively affect your systems (i.e., window of compromise).

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

Identifying the differing levels of exploitability should help an organization prioritize the actions it should take to enhance its IT security.

The purpose of the risk assessment is to help organizations document potential security vulnerabilities, threats, and risks.

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 originate from employees. Although most workers aren't malicious, they often either forget security best practices or don't know exactly what they're required to do.

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

By holding employees accountable, you can protect your business and customers more effectively.

Employees need to be given specific rules and regular training. A security awareness program that includes regular training (e.g., brief monthly training) 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:

- **Set monthly training meetings:** 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.
- **Create incentives:** Reward your employees for being proactive.
- **Regularly test employees:** Create an environment where employees aren't afraid to report suspicious behavior.

TIPS FROM AN AUDITOR

REQUIREMENT 12: PCI COMPLIANCE BASICS

First, make PCI compliance a regular business practice. If you view compliance as a once-a-year task, you'll probably struggle and slip in and out of compliance regularly. Your PCI compliance efforts should encourage a cultural shift to common corporate culture practices. You can't bypass the process.

Second, document everything, including all processes, policies, roles, and responsibilities. Additionally, make sure all service providers sign PCI DSS compliance business agreements. For each service provider you use, document their PCI DSS responsibilities. Ensure your service providers are PCI compliant at least on a yearly basis.

Your security policies and procedures should be living documents.

Finally, conduct a risk assessment. Your environment may require going beyond PCI requirements to secure your payment data. That's why you need an annual process review, documentation of the review, regular risk assessments, and updated policies.

When conducting your risk assessment, look at what's happening in your industry and analyze common breaches. Build your policy around what you discover.

JEN STONE
QSA | CISSP | CISA | MSCIS

REQUIREMENT 12 IT CHECKLIST

CORPORATE POLICY AND DOCUMENTATION

*Assigned to:*_____

*Assignment date:*_____

*Completion date:*_____

THINGS YOU WILL NEED TO HAVE:

- [ ] Written compliance and security policies
- [ ] Charter for PCI DSS compliance program
- [ ] Service providers must perform quarterly reviews to confirm policies and procedures are being followed

THINGS YOU WILL NEED TO DO:

- [ ] Ensure that each employee working in the CDE completes annual security awareness training. (12.6, 12.6.1)

THINGS YOU MAY NEED TO DO:

- [ ] Create a company policy documenting all critical devices and services within the payment processing environment. Some examples include laptops, tablets, email and Internet usage, remote access, and wireless access technologies. This policy should include acceptable uses and storage of these technologies. The general purpose of this policy is to thoroughly explain each employee's role in the CDE. Review your policy and lists annually. (12.1-12.4)
- [ ] Create and document an approval process for allowing employee access to technologies. Keep lists readily available and review them annually. (12.1-12.4)

- [ ] Create an incident response plan in the event that cardholder data is compromised (12.10.1). Your plan should include the following:
  - [ ] Roles and contact strategies in the event of compromise
  - [ ] Specific incident response procedures
  - [ ] Business continuity and recovery procedures
  - [ ] Data backup processes
  - [ ] Analysis of legal requirements in reporting possible compromise
  - [ ] Critical systems coverage and response plans
  - [ ] Notification of merchant processor and payment card brands
  - [ ] Create and update a current list of third-party service providers (e.g., your IT provider, credit card machine vendor, and credit card receipt shredder)
- [ ] The following will need to be completed annually regarding your service providers (12.8, 12.8.1):
  - [ ] Establish a process for engaging with third-party providers. Best practice would be to contact them by phone rather than taking inbound calls. Work by appointment with service providers onsite. (12.8.3)
  - [ ] Obtain or update a written agreement from third-party providers acknowledging their responsibility for the cardholder information they possess. Ensure they are following PCI compliance requirements themselves. (12.8.2)
  - [ ] Establish a process for engaging new providers, including research prior to selecting a provider.

HOW TO PREPARE FOR A DATA BREACH

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 brand in the wake of a data breach's potentially devastating hold on brand reputation.

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

INCIDENT RESPONSE PLAN OVERVIEW

INCIDENT RESPONSE PLAN BASICS

Unfortunately, every organization 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:

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+**

To help minimize a data breach, establish well-executed incident response plan, which can help minimize breach impact, reduce fines, decrease negative press, and help you get back to normal operations more quickly.

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 incident response 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.

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

INCIDENT RESPONSE PHASE TIMELINE

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.

PHASE 2: IDENTIFY

Identification (or detection) is the 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-virus 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.

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

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, it allows a forensic investigator to evaluate untouched systems. This is easier to do in virtual server environments but can be costly otherwise.
- 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, please 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 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 or a third party do this, you need 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).

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, you need 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

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. This 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 are affected by the breach?
- How was it discovered?
- Is any other personal 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, and what will you do to prevent this from happening 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 executives.

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:

- Process for disconnecting from the Internet (e.g., who is responsible to decide whether or not you disconnect)
- System configuration diagrams that include information (e.g., 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 OS
- 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 minimizing the damage from a data breach.

STEP 1: IDENTIFY AND PRIORITIZE ASSETS

Start by identifying and documenting where your organization keep 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 importance and highest risk, 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 Internet 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 blunders 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

You need to 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 including a specific responsibility to manage the 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 then be 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 and regularly trained on your incident response plan and know what they're expected to do after a data breach.

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 or what's known as tabletop exercises. Tabletop exercises allow employees to learn about 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 table exercise, incident response team members discuss response roles in hypothetical situations. A discussion-based 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 some 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 addition to your malware prevention controls. New malware comes out so frequently that you can't rely only on anti-virus software to protect your systems. It often takes months for a signature of newly detected malware to make it into malware signature files, allowing it to be detected by anti-virus software.

Configure FIM software to watch critical file directories for changes. 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 make sure you know what those files are. If the change was known (e.g., a system update), then you don't need to worry. If not, chances are you have new malware that could not be recognized and can now be dealt with.

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

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

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

INSTALL INTRUSION DETECTION AND PREVENTION SYSTEMS

One reason that data breaches are so prevalent is a lack of implemented security tools 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 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, use an intrusion prevention system (IPS). An IPS can prevent and block many detected intrusions, as well as monitor network activity for malicious activities, log this information, and report it. Intrusion prevention systems can drop malicious packets, block traffic from the malicious source address, and resetting 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

PCI DSS BUDGET

The cost of PCI compliance depends entirely on your organization. Here are a few variables that will factor in to 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 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, and the model of back-end servers 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:

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 companies with various groups (e.g., networking, IT, HR, risk) expecting other departments to take charge of PCI compliance. Other times, organizations expect a QSA to be the PCI project manager, which is not feasible.

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 that 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 here is how it will damage our brand." Consider asking marketing or accounting teams for help delivering the message in more bottom-line terms.

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

TIPS FROM AN AUDITOR

PCI DSS RESPONSIBILITIES AND CHALLENGES

The PCI DSS does not change based on the size of the company or their cardholder data environment, but PCI challenges can vary significantly.

It has been my experience that 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 the time to document procedures. Unfortunately, it's not uncommon to perform a renewal assessment where they 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.

To help address some of these concerns, requirement 12.4.1 requires service providers 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 (requirement 12.4.1). Additionally, they should implement internal audit procedures to ensure security practices are properly in place throughout the year (requirement 10.8 and 12.11).

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.

If organizations do not take the necessary time and effort to respond to genuine alerts, the only thing they will gain are checkmarks on their SAQ.

JEN STONE
QSA | CISSP | CISA | MSCIS

CONTRIBUTORS

MATT HALBLEIB

JEN STONE

GEORGE MATEAKI

MICHAEL SIMPSON

MICHAEL MAUGHAN

MICHAEL OHRAN

GARY GLOVER

DAVID PAGE

TREVOR HANSEN

MARK MINER

WINN OAKEY

BRAD CALDWELL

REBECCA CAMEAU

MARJ ELDARD

ELLEN BAHR

DAVID ELLIS

BRADLEY SMITH

JOSHUA BRANDEBERRY

JACOB THAYNE

SAM MONSIVAIS

WHITNEY TAYLOR

PARKER NELSON

BRAD NELSON

MELINDA HOWLETT

JEFF MCKENNA

KAI WHITAKER

CHUCK BRAILSFORD

DON ROBERTSON

TYLER FARR

FORREST BARTH

SIDNIE ANDERSON

RICH BUSHELL

JON CLARK

RYAN RUNNING

ANDREW GARRETT

HIEDI BLACKWELDER

MEAGAN ELGUERA

ERIC SMITH

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: The time that 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.

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.

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

Multi-factor Authentication (MFA): At least 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 agency that measures standards and maintains the National Vulnerability Database (NVD).

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

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.

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*)

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.

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.

ABOUT SECURITYMETRICS

We help customers close data security and compliance gaps to avoid data breaches. We provide managed data security services and are certified to help you achieve the highest data security and compliance standards.

We are a PCI certified Approved Scanning Vendor (ASV), Qualified Security Assessor (QSA), Certified Forensic Investigator (PFI), and Managed Security provider with 18 years of data security experience. From local shops to some of the world's largest brands, we help businesses achieve data security through managed services and compliance mandates (PCI, HIPAA, GDPR). 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-audit

securityMETRICS®