PCI DSS v4.0.1 March 31st Deadline: Essential Steps for Fuel Retailers

February 13, 2025

Your Host:
Casey Brant

Standards Coordinator
Conexxus, Inc.

Your Moderator:
Phil Stead - CISSP, CISM, PCI-QIR, PCIP

VP of Sales
Acumera, Inc

Agenda

□ Housekeeping

□ About Conexxus

□ Presenters

□ Presentation

□ Q&A

Housekeeping

This webinar is being recorded and will be made available on Conexxus365.org

Participants

□ Ask questions via webinar interface

□ Please, no vendor specific questions

4 Our webinars may be used toward PCI continuing education credits. Please contact 365@conexxus.org for questions regarding a certificate of webinar attendance for qualifying live events.

Interested in speaking or sponsoring a Conexxus365 event?
Contact 365@conexxus.org to discuss upcoming opportunities with our team.

Disclaimer

Conexxus does not endorse any products or services that may be described or mentioned in this presentation.

The views and opinions expressed in this presentation are solely those of the speakers and not of Conexxus.

By hosting this webinar, Conexxus is not providing any legal advice; if you have any questions about legal issues raised or discussed, you should seek the assistance of attorneys who are competent in that area.

Thank you to our 2025 Annual Diamond Sponsors!

Acumera®

AiFA LABS

armor™ SAFE TECHNOLOGIES

Bulloch TECHNOLOGIES | DOVER® FUELING SOLUTIONS | AvaLAN® NETWORKS

Bluefin®

FIELD ADVANTAGE

HUGHES® An EchoStar Company

invenco by GVR

K3DES

Mako® NETWORKS

NACS®

NCR VOYIX

About Conexxus

- We are an independent, non-profit, member driven technology organization

We set **standards**…

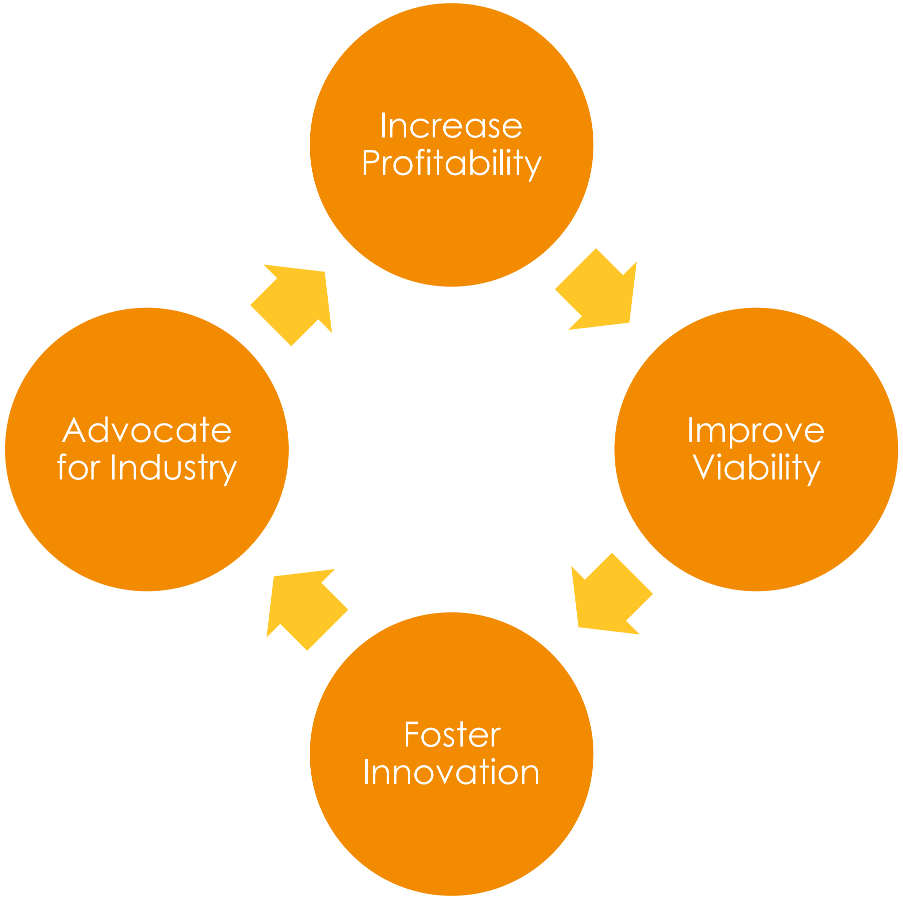
- Data exchange
- Security
- Mobile commerce

We provide **vision**

- Identify emerging tech/trends

We **advocate** for our industry

- Technology is policy



Connect with Conexxus

CONEXXUS 365

www.conexxus365.org

365@conexxus.org

CONEXXUS

solve forward

www.conexxus.org

info@conexxus.org

LinkedIn

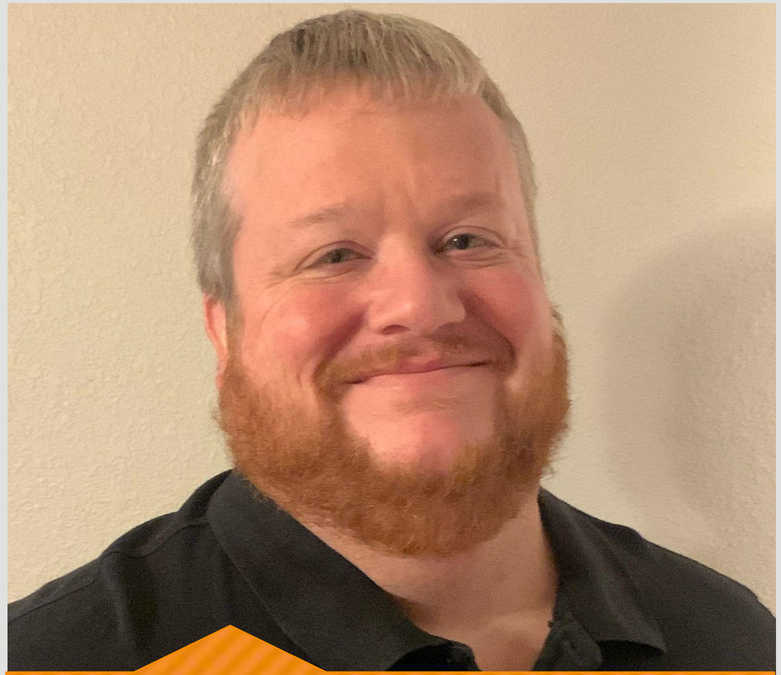
@conexxus.org

PCI DSS v4.0.1 March 31st Deadline: Essential Steps for Fuel Retailers

February 13, 2025

Ashwin Swamy

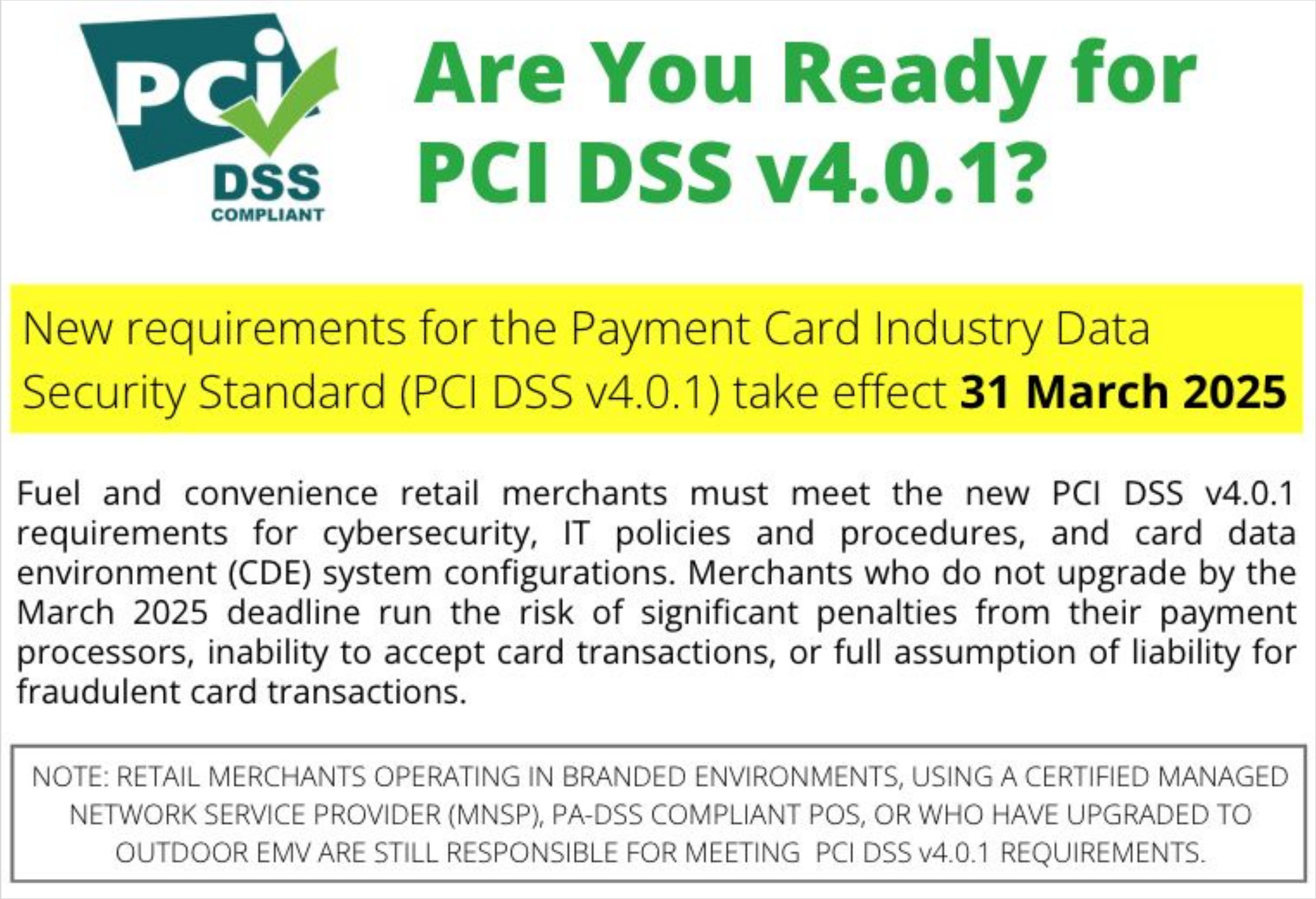
CEO
Omega ATC
ashwin.swamy@omegaatc.com
636-557-6000



Gregory DeClue

Cyber Operations Manager
Omega ATC
greg.declue@omegaatc.com
636-557-6000

PCI DSS v4.0.1 Future-dated Requirements



Are You Ready for PCI DSS v4.0.1?

New requirements for the Payment Card Industry Data Security Standard (PCI DSS v4.0.1) take effect **31 March 2025**

Fuel and convenience retail merchants must meet the new PCI DSS v4.0.1 requirements for cybersecurity, IT policies and procedures, and card data environment (CDE) system configurations. Merchants who do not upgrade by the March 2025 deadline run the risk of significant penalties from their payment processors, inability to accept card transactions, or full assumption of liability for fraudulent card transactions.

NOTE: RETAIL MERCHANTS OPERATING IN BRANDED ENVIRONMENTS, USING A CERTIFIED MANAGED NETWORK SERVICE PROVIDER (MNSP), PA-DSS COMPLIANT POS, OR WHO HAVE UPGRADED TO OUTDOOR EMV ARE STILL RESPONSIBLE FOR MEETING PCI DSS v4.0.1 REQUIREMENTS.

- ✓ **Up-to-date with emerging threats**
- ✓ **Greater flexibility**
- ✓ **52 New Requirements**
- ✓ **Applies to All Merchant Levels**

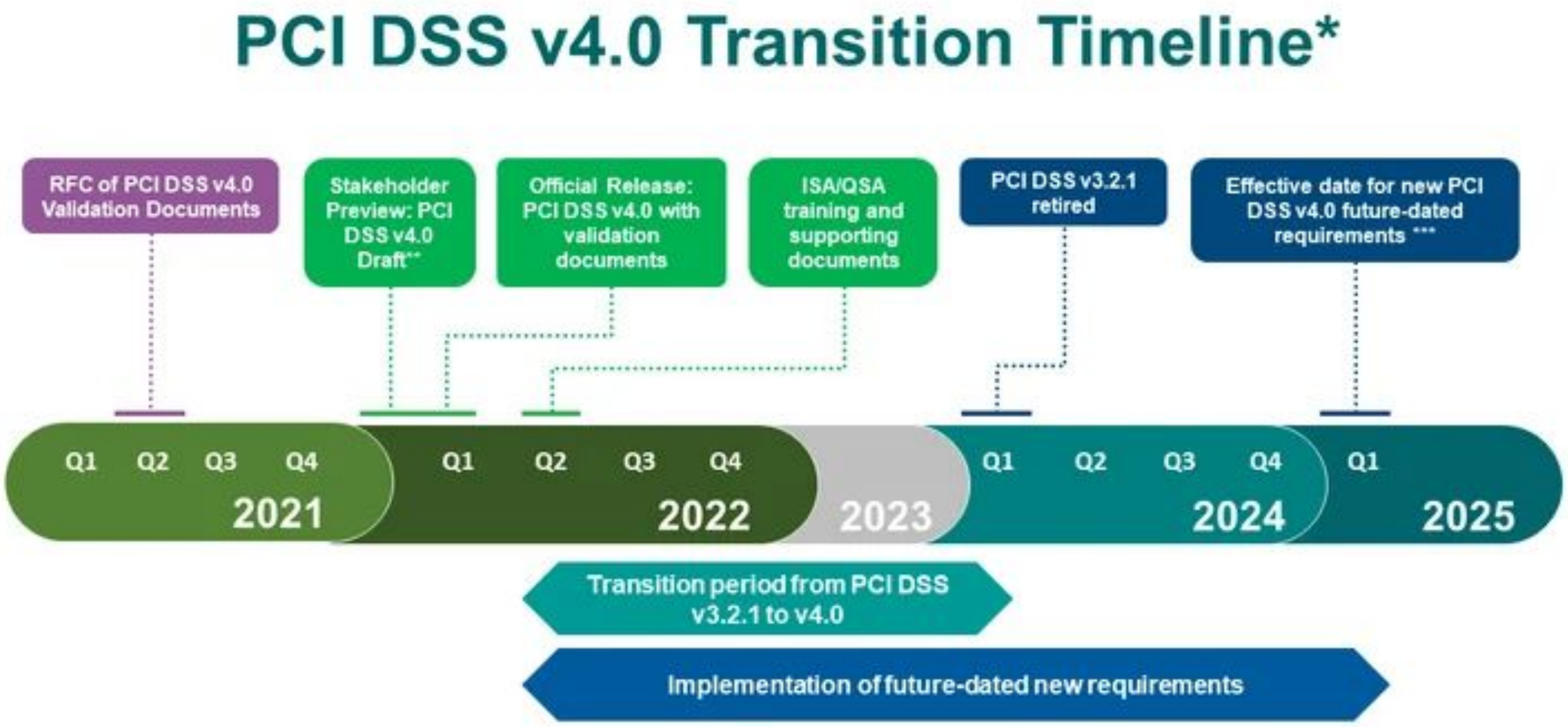
PCI DSS v4.0.1 Future-dated Requirements

PCI Security Standards Council

Payment Card Industry
Data Security Standard

Summary of Changes from
PCI DSS Version 3.2.1 to 4.0

Revision 1
May 2022



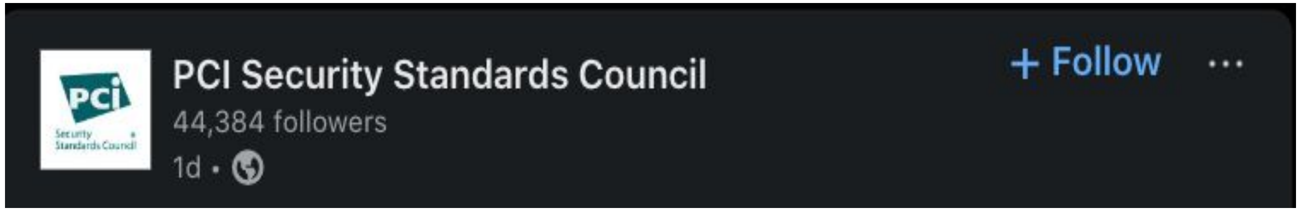
PCI DSS v4.0 Transition Timeline*

- RFC of PCI DSS v4.0 Validation Documents
- Stakeholder Preview: PCI DSS v4.0 Draft**
- Official Release: PCI DSS v4.0 with validation documents
- ISA/QSA training and supporting documents
- PCI DSS v3.2.1 retired
- Effective date for new PCI DSS v4.0 future-dated requirements ***

Transition period from PCI DSS v3.2.1 to v4.0

Implementation of future-dated new requirements

PCI DSS v4.0.1 - Latest Announcements



PCI Security Standards Council

44,384 followers

1d •

After thorough consideration and review of industry stakeholder feedback, PCI SSC is making the following updates to SAQ A:

- Removal of PCI DSS Requirements 6.4.3 and 11.6.1 for payment page security, and Requirement 12.3.1 for a Targeted Risk Analysis to support Requirement 11.6.1.

- Addition of an Eligibility Criteria for merchants to “confirm their site is not susceptible to attacks from scripts that could affect the merchant’s e-commerce system(s).”

PCI Security Standards Council
Important Updates Announced for Merchants Validating to Self-Assessment Questionnaire A

Are we ready to go toe-to-toe against today’s threats?

PCI DSS v4.0.1 prepares merchants for today’s threats - AI-based attacks, new forms of malware, more sophisticated hackers, larger attack surface

How do we bring alignment in a multi-vendor environment?

Every party has to get aligned - fast!

PCI DSS COMPLIANT

Service Contractors

MNSPs

Management

TPSPs

POS Vendors

IT Staff

Frontline Workers

Upgrade to PCI DSS v4.0.1 in three phases!

- ✓ DEFINE YOUR SCOPE
- ✓ IMPLEMENT SECURITY CONTROLS
- ✓ IMPLEMENT POLICIES & PROCEDURES

1 - Define Your Scope & Responsibilities

✓ DEFINE YOUR SCOPE

CREATE YOUR ORGANIZATIONAL PROFILE
Map out all retail technology formats in your enterprise

VERIFY ROLES AND RESPONSIBILITIES
Engage with your third-party service providers (TPSPs) and define who is responsible for each PCI requirement

DEFINE YOUR CARDHOLDER DATA ENVIRONMENT (CDE)
Identify all systems and network segments involved in storing, processing, or transmitting cardholder data, and “connected-to” systems

VERIFY NEW PCI CONFIGURATIONS
Check to make sure that systems are updated to the new PCI configuration requirements (passwords, MFA, etc.)

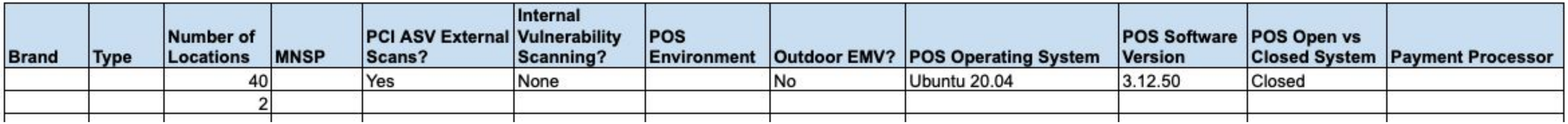
1 - Define Your Scope & Responsibilities

DEFINE YOUR SCOPE

CREATE YOUR ORGANIZATIONAL PROFILE

Map out all retail technology formats in your enterprise

- Brands, Retail Technology Formats (POS, payment processor, MNSP), Merchant IDs, Verifying Merchant Supplier / Operator Agreements
- Identify Internal Roles and Stakeholders



Brand	Type	Number of Locations	MNSP	PCI ASV External Scans?	Internal Vulnerability Scanning?	POS Environment	Outdoor EMV?	POS Operating System	POS Software Version	POS Open vs Closed System	Payment Processor
		40		Yes	None		No	Ubuntu 20.04	3.12.50	Closed	
		2									

1 - Define Your Scope & Responsibilities

DEFINE YOUR SCOPE

DEFINE YOUR CARDHOLDER DATA ENVIRONMENT (CDE)

Identify all systems and network segments involved in storing, processing, or transmitting cardholder data

12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment.

At a minimum, the scoping validation includes: () Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). () Updating all data-flow diagrams per Requirement 1.2.4. () Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. () Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. () Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. () Identifying all connections from third-party entities with access to the CDE. () Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.

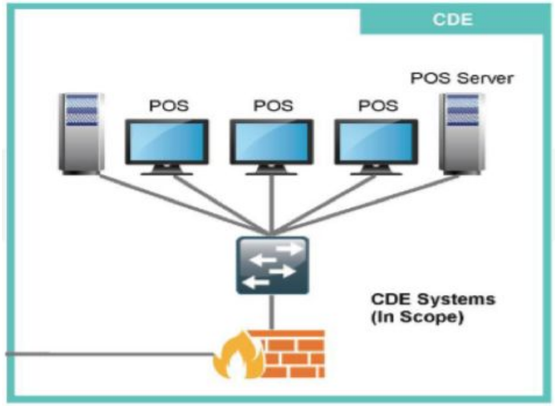
1 - Define Your Scope & Responsibilities

✓ DEFINE YOUR SCOPE

DEFINE YOUR CARDHOLDER DATA ENVIRONMENT (CDE)

Identify all systems and network segments involved in storing, processing, or transmitting cardholder data

12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment.



Network and data flow diagrams are cool!

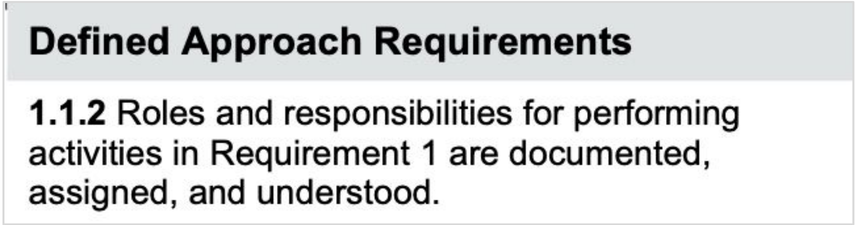
(Do better than this one…though something is better than nothing!)

Engage Your Third Parties (TPSPs)!

DEFINE YOUR SCOPE

VERIFY ROLES AND RESPONSIBILITIES

"X.1.2" for each PCI requirement



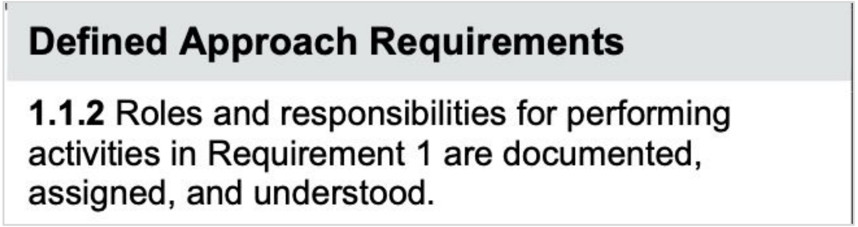
Defined Approach Requirements
1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.

- Start with your brands, technology vendors (POS, MNSP), payment processors, and service contractors
- Get an updated R&R document and service agreement from each TPSP - what PCI controls are they taking responsibility for?
- Get a PCI DSS v4.0.1 "Attestation of Compliance" (AOC) from each TPSP, or an R&R document that indicates that they are performing the activities required by PCI DSS v4.0.1
- Incident / Breach Notification Policies & SLAs

Engage Your Third Parties (TPSPs)!

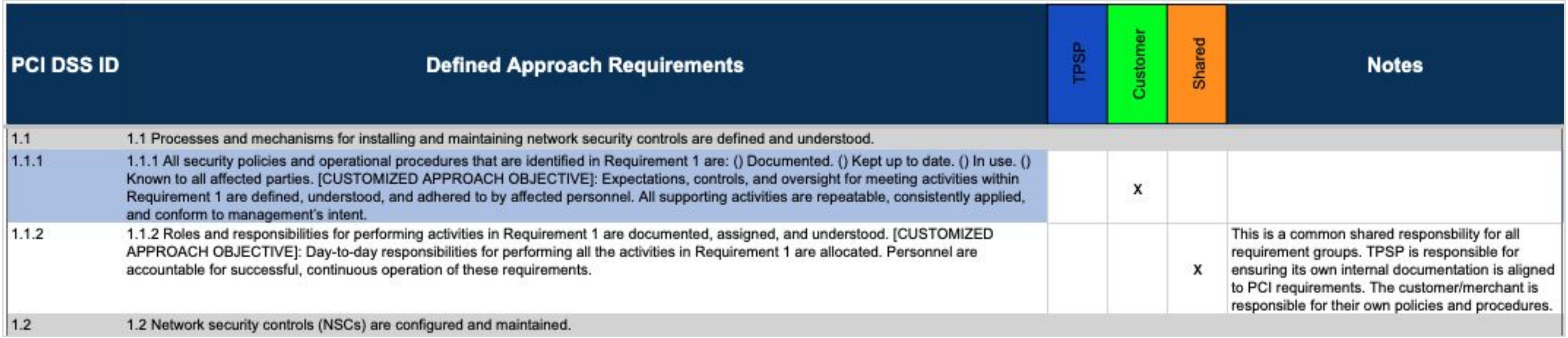
DEFINE YOUR SCOPE

VERIFY ROLES AND RESPONSIBILITIES
"X.1.2" for each PCI requirement



Defined Approach Requirements

1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.



PCI DSS ID	Defined Approach Requirements	TPSP	Customer	Shared	Notes
1.1	1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.				
1.1.1	1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: () Documented. () Kept up to date. () In use. () Known to all affected parties. [CUSTOMIZED APPROACH OBJECTIVE]: Expectations, controls, and oversight for meeting activities within Requirement 1 are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		x		
1.1.2	1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood. [CUSTOMIZED APPROACH OBJECTIVE]: Day-to-day responsibilities for performing all the activities in Requirement 1 are allocated. Personnel are accountable for successful, continuous operation of these requirements.			x	This is a common shared responsbility for all requirement groups. TPSP is responsible for ensuring its own internal documentation is aligned to PCI requirements. The customer/merchant is responsible for their own policies and procedures.
1.2	1.2 Network security controls (NSCs) are configured and maintained.				

Ensure your systems are updated to the new configuration standards

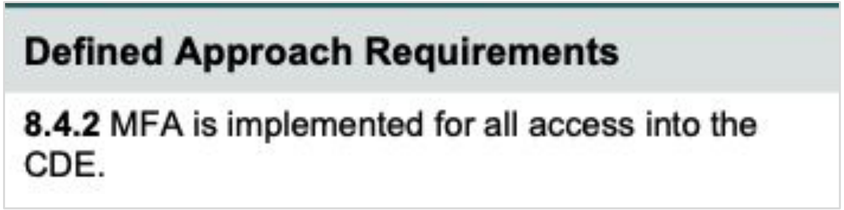
DEFINE YOUR SCOPE

VERIFY NEW PCI CONFIGURATIONS

Check to make sure that systems are updated to the new PCI configuration requirements (passwords, MFA, etc.)

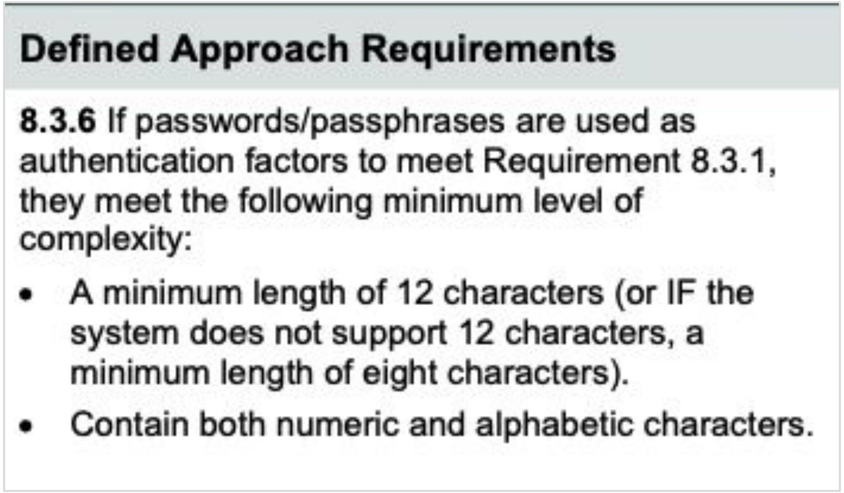
Identify all users with access to systems in scope

- Internal or Third Party
- Role levels by business use (least privileged access)
- Information Security Policy
- Verify Users / Remove inactive users
- Ensure enforcement of multifactor authentication (PCI DSS requirement 8.4.2, 8.5.1)



Defined Approach Requirements

8.4.2 MFA is implemented for all access into the CDE.



Defined Approach Requirements

8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:

- A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).
- Contain both numeric and alphabetic characters.

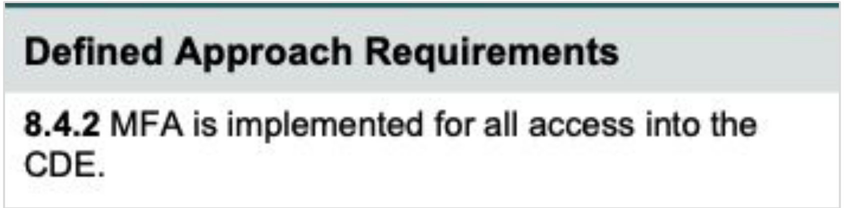
Ensure your systems are updated to the new configuration standards

✓ DEFINE YOUR SCOPE

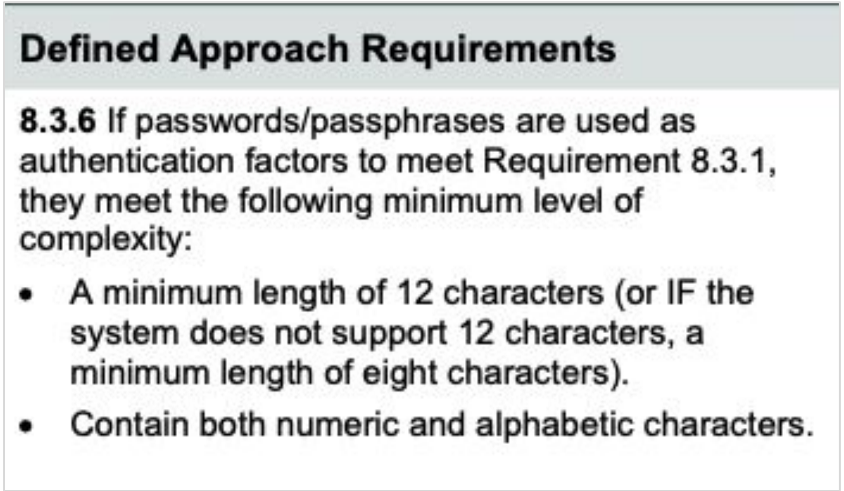
VERIFY NEW PCI CONFIGURATIONS

Check to make sure that systems are updated to the new PCI configuration requirements (passwords, MFA, etc.)

- New Password Complexity (PCI DSS requirement 8.3.6)
- Passwords must be at least 12 characters long and include a mixture of special characters, uppercase, and lowercase letters.
- Passwords must be changed every 90 days



Defined Approach Requirements
8.4.2 MFA is implemented for all access into the CDE.



Defined Approach Requirements

8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:

- A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).
- Contain both numeric and alphabetic characters.

2 - Implement Your Security Controls

- ✓ DEFINE YOUR SCOPE
- ✓ IMPLEMENT SECURITY CONTROLS
- ✓ IMPLEMENT POLICIES & PROCEDURES

2 - Implement Your Security Controls

- ✓ DEFINE YOUR SCOPE
- ✓ IMPLEMENT SECURITY CONTROLS
- ✓ IMPLEMENT POLICIES & PROCEDURES

Targeted Risk Analysis
(PCI DSS requirement 12.3.1)

Firewall Rules and Segmentation
(PCI DSS requirement 1)

User access & system configurations
(PCI DSS requirement 7 and 8)

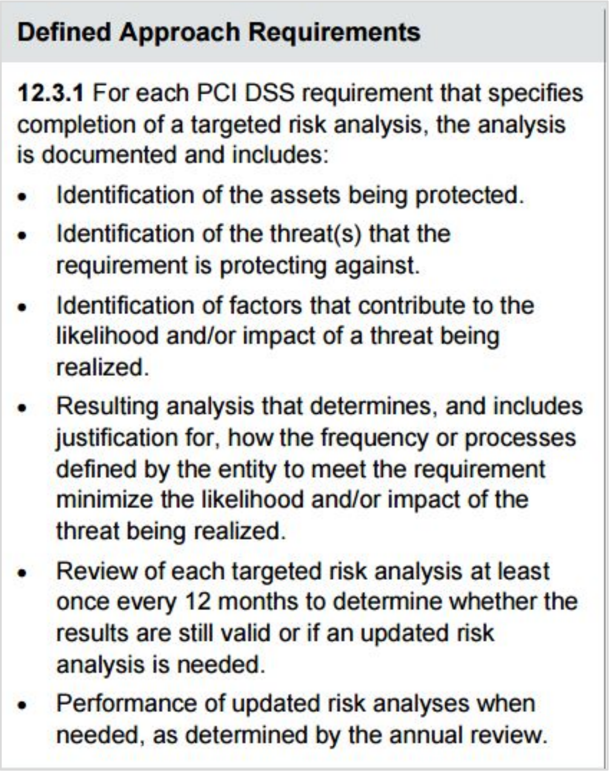
Protect systems from malicious software
(PCI DSS requirement 5)

Continuous Monitoring
(PCI DSS requirement 10, 11.5.2)

Authenticated Vulnerability Scanning
(PCI DSS requirement 11.3.1)

The PCI DSS v4.0.1 Targeted Risk Analysis

IMPLEMENT SECURITY CONTROLS

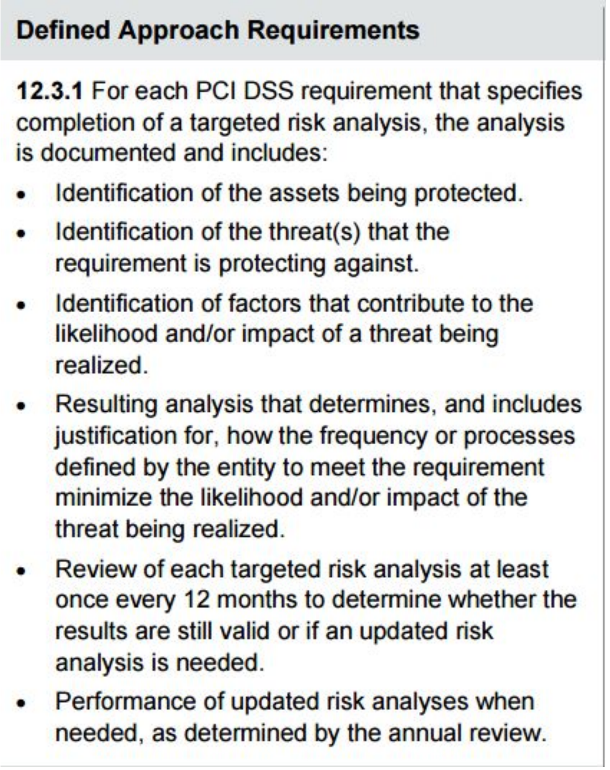


Defined Approach Requirements
12.3.1 For each PCI DSS requirement that specifies completion of a targeted risk analysis, the analysis is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how the frequency or processes defined by the entity to meet the requirement minimize the likelihood and/or impact of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review.

Just Published: PCI DSS v4.x Targeted Risk Analysis Guidance

The TRA gives merchants flexibility

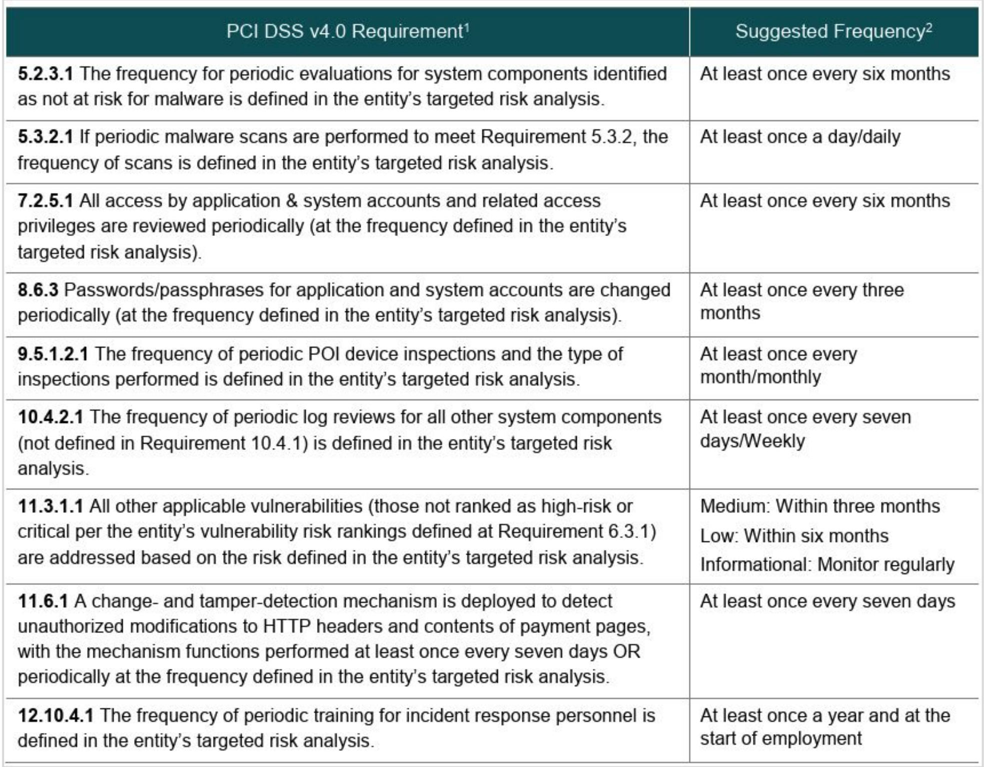
IMPLEMENT SECURITY CONTROLS



Defined Approach Requirements

12.3.1 For each PCI DSS requirement that specifies completion of a targeted risk analysis, the analysis is documented and includes:

- Identification of the assets being protected.
- Identification of the threat(s) that the requirement is protecting against.
- Identification of factors that contribute to the likelihood and/or impact of a threat being realized.
- Resulting analysis that determines, and includes justification for, how the frequency or processes defined by the entity to meet the requirement minimize the likelihood and/or impact of the threat being realized.
- Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.
- Performance of updated risk analyses when needed, as determined by the annual review.



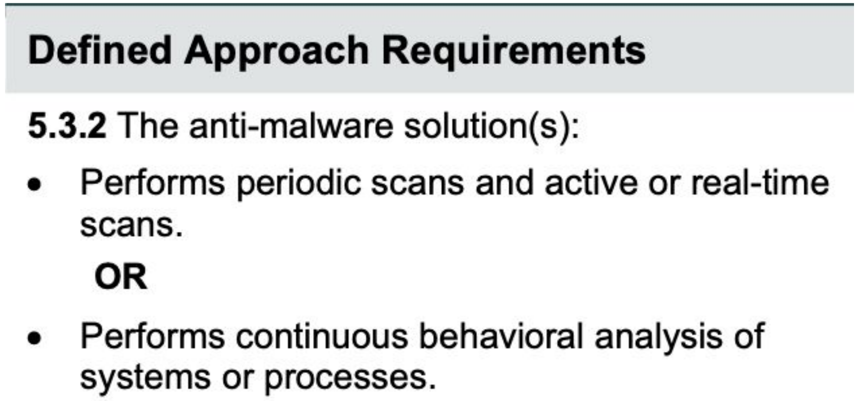
PCI DSS v4.0 Requirement[1]	Suggested Frequency[2]
5.2.3.1 The frequency for periodic evaluations for system components identified as not at risk for malware is defined in the entity's targeted risk analysis.	At least once every six months
5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis.	At least once a day/daily
7.2.5.1 All access by application & system accounts and related access privileges are reviewed periodically (at the frequency defined in the entity's targeted risk analysis).	At least once every six months
8.6.3 Passwords/passphrases for application and system accounts are changed periodically (at the frequency defined in the entity's targeted risk analysis).	At least once every three months
9.5.1.2.1 The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis.	At least once every month/monthly
10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis.	At least once every seven days/Weekly
11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are addressed based on the risk defined in the entity's targeted risk analysis.	Medium: Within three months Low: Within six months Informational: Monitor regularly
11.6.1 A change- and tamper-detection mechanism is deployed to detect unauthorized modifications to HTTP headers and contents of payment pages, with the mechanism functions performed at least once every seven days OR periodically at the frequency defined in the entity's targeted risk analysis.	At least once every seven days
12.10.4.1 The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis.	At least once a year and at the start of employment

Install & Configure Endpoint Security

IMPLEMENT SECURITY CONTROLS

Ensure proper endpoint security is in place (PCI DSS requirement 5.2.2, 5.3.1, 5.3.2...)

- All system components in the CDE with an OS
- Removable Media Scanning (PCI DSS requirement 5.3.3)
- File Integrity Monitoring (PCI DSS requirement 11.5.2)
- Anti-malware with Behavioral Detection
- Continuous Monitoring (PCI DSS requirement 10)



Defined Approach Requirements

5.3.2 The anti-malware solution(s):

- Performs periodic scans and active or real-time scans.

  OR

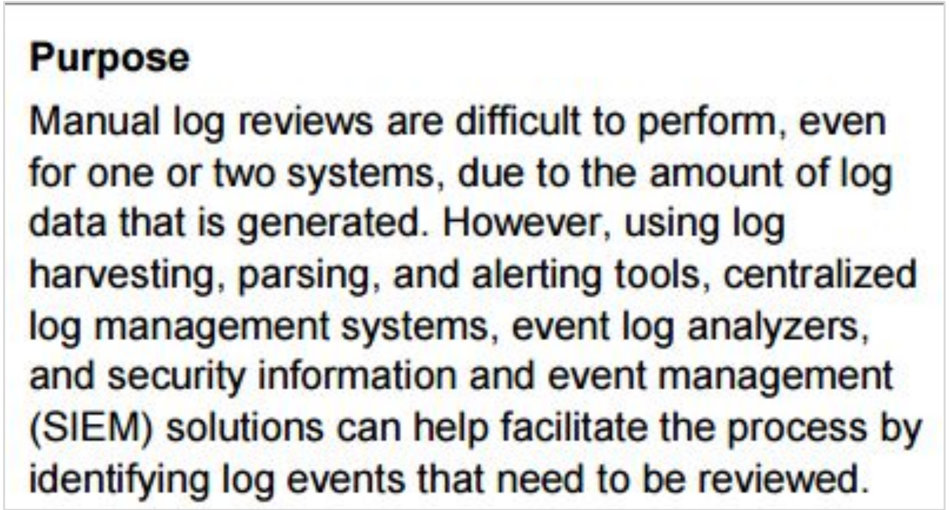
- Performs continuous behavioral analysis of systems or processes.

Designate a syslog server for logging

IMPLEMENT SECURITY CONTROLS

Ensure proper endpoint security is in place (PCI DSS requirement 5.2.2, 5.3.1, 5.3.2…)

- All system components in the CDE with an OS
- Removable Media Scanning (PCI DSS requirement 5.3.3)
- File Integrity Monitoring (PCI DSS requirement 11.5.2)
- Anti-malware with Behavioral Detection
- Continuous Monitoring (PCI DSS requirement 10)



Purpose

Manual log reviews are difficult to perform, even for one or two systems, due to the amount of log data that is generated. However, using log harvesting, parsing, and alerting tools, centralized log management systems, event log analyzers, and security information and event management (SIEM) solutions can help facilitate the process by identifying log events that need to be reviewed.

Authenticated Scanning? Really?

✓ IMPLEMENT SECURITY CONTROLS

Authenticated Scanning (PCI DSS requirement 11.3.1.2)

- All Vulnerabilities Matter
- Service accounts will have to be added to each system in the CDE.
- Merchants will be required to have 4 *consecutive quarters* of passing scans.
- Vulnerabilities should be classified by a qualitative *risk* rating (PCI DSS requirement 6.3.1)
- The targeted risk analysis (TRA) can help provide flexibility for remediation timeframe.
- The right risk and vulnerability data management strategy can help make this manageable.

Implement policies & procedures organization-wide

- ✓ DEFINE YOUR SCOPE
- ✓ IMPLEMENT SECURITY CONTROLS
- ✓ IMPLEMENT POLICIES & PROCEDURES

Implement policies & procedures organization-wide

✓ **DEFINE YOUR SCOPE**

✓ **IMPLEMENT SECURITY CONTROLS**

✓ **IMPLEMENT POLICIES & PROCEDURES**

Security Awareness Training
(PCI DSS requirement 12.6.1)

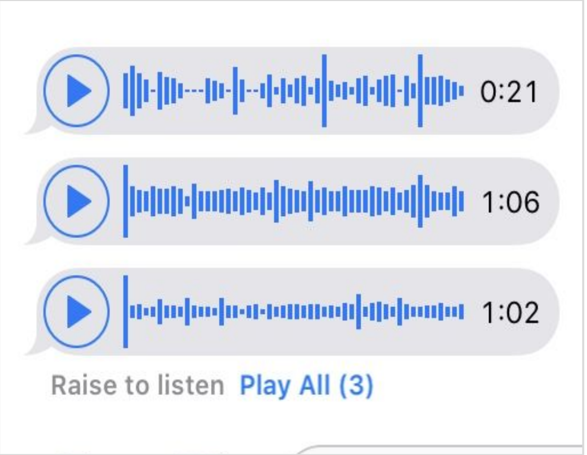
Incident Response Planning
(PCI DSS requirement 12.10.1)

Information Security Policy
(PCI DSS requirement x.1.1)

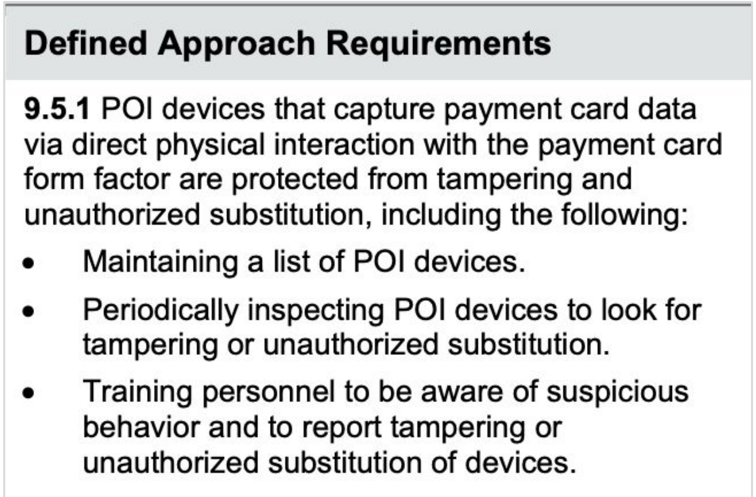
3 - Policies & Procedures | security awareness

Security awareness training (PCI DSS requirement 12.6, 9.5) must become an organization-wide activity, **including frontline employees and management.**

Human error is the primary entry point for hackers.



Deepfake Voice

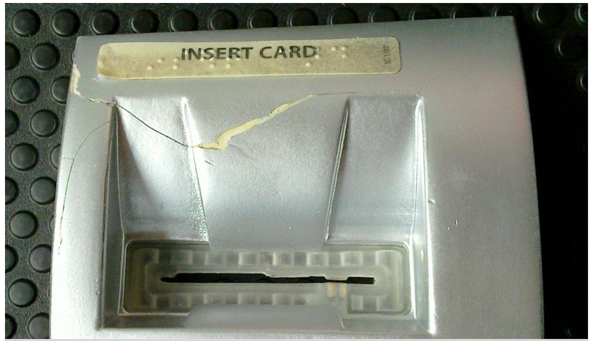


Defined Approach Requirements

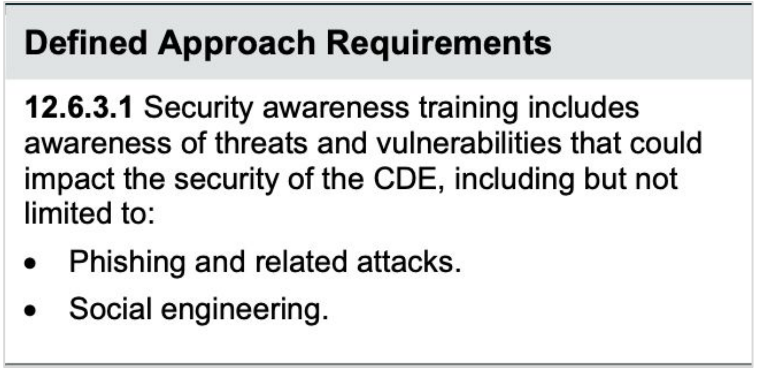
9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:

- Maintaining a list of POI devices.
- Periodically inspecting POI devices to look for tampering or unauthorized substitution.
- Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.

Deepfake Video



Skimmers



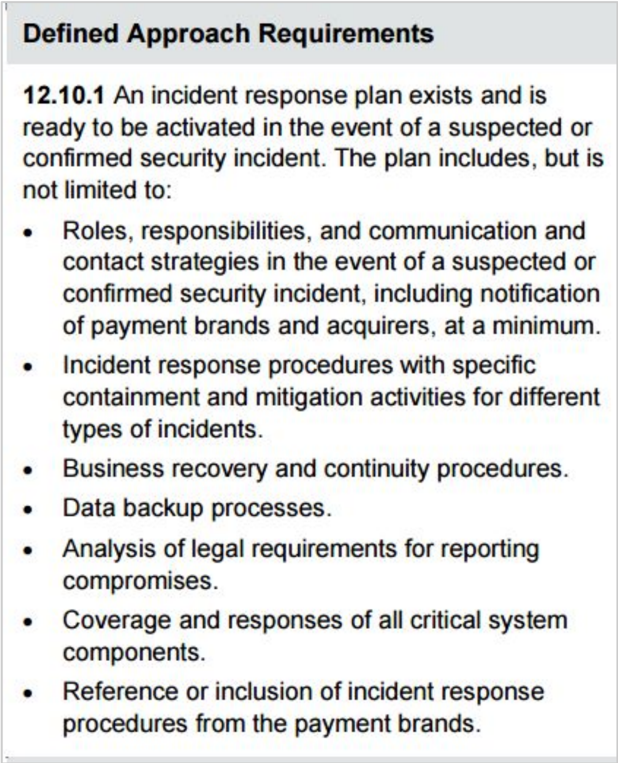
Defined Approach Requirements

12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to:

- Phishing and related attacks.
- Social engineering.

3 - Policies & Procedures | incident response

Review PCI DSS requirement 12.10



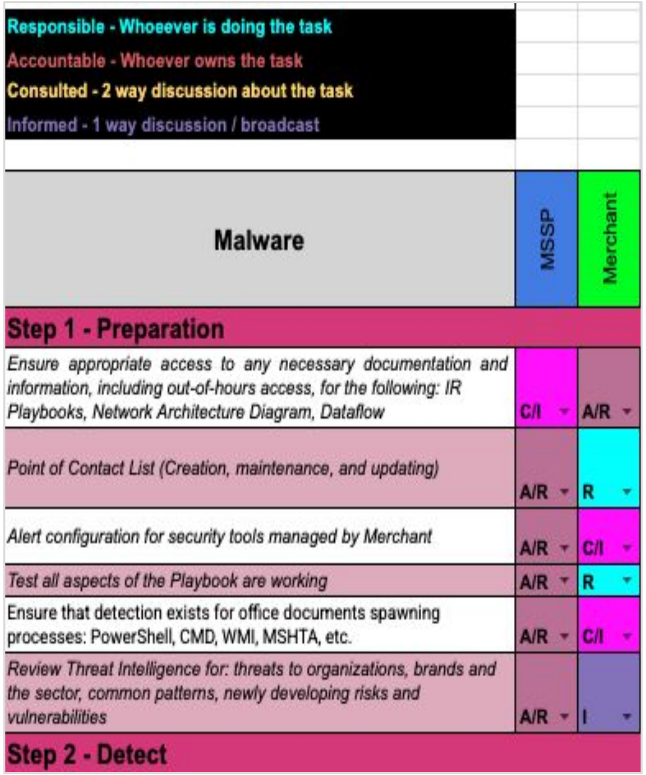
Defined Approach Requirements

12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to:

- Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.
- Incident response procedures with specific containment and mitigation activities for different types of incidents.
- Business recovery and continuity procedures.
- Data backup processes.
- Analysis of legal requirements for reporting compromises.
- Coverage and responses of all critical system components.
- Reference or inclusion of incident response procedures from the payment brands.

Engage TPSPs and Stakeholders

Rehearse Playbooks for Each Incident Type



Responsible - Whoeever is doing the task

Accountable - Whoever owns the task

Consulted - 2 way discussion about the task

Informed - 1 way discussion / broadcast

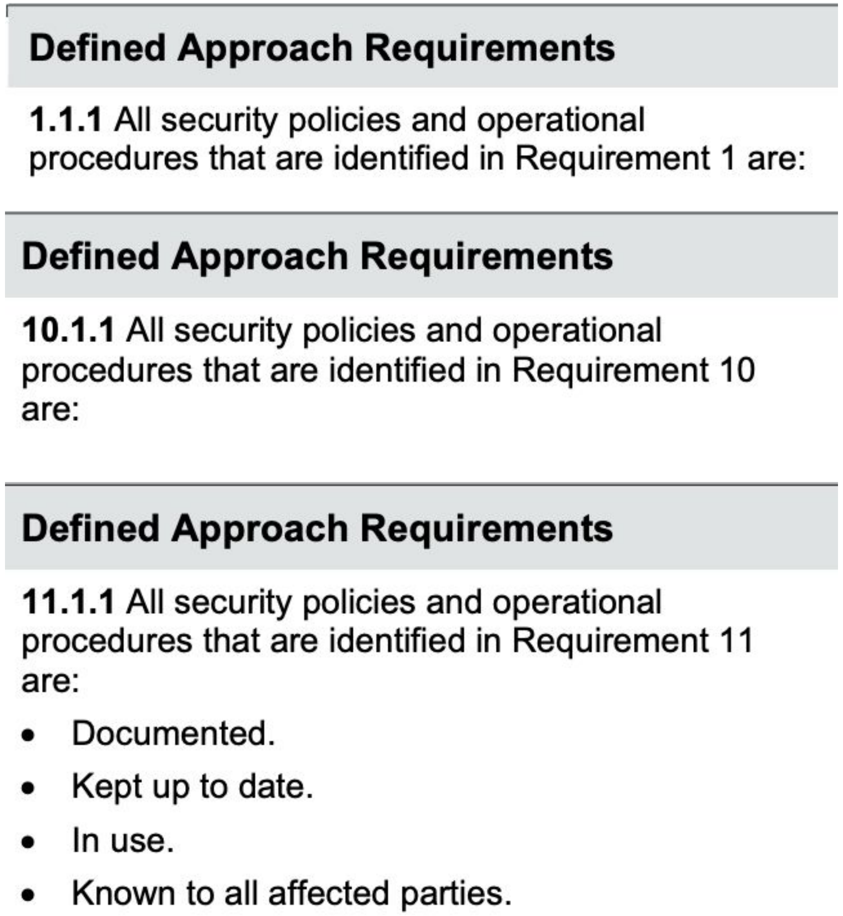
Malware	MSSP	Merchant
Step 1 - Preparation		
Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following: IR Playbooks, Network Architecture Diagram, Dataflow	C/I	A/R
Point of Contact List (Creation, maintenance, and updating)	A/R	R
Alert configuration for security tools managed by Merchant	A/R	C/I
Test all aspects of the Playbook are working	A/R	R
Ensure that detection exists for office documents spawning processes: PowerShell, CMD, WMI, MSHTA, etc.	A/R	C/I
Review Threat Intelligence for: threats to organizations, brands and the sector, common patterns, newly developing risks and vulnerabilities	A/R	I
Step 2 - Detect		

CONEXXUS 365

CONEXXUS solve forward

3 - Policies & Procedures | governance

PCI DSS requirement x.1.1 for each requirement asks merchants to develop an information security policy governing operational procedures and security policies for each requirement, with ongoing oversight and change management.



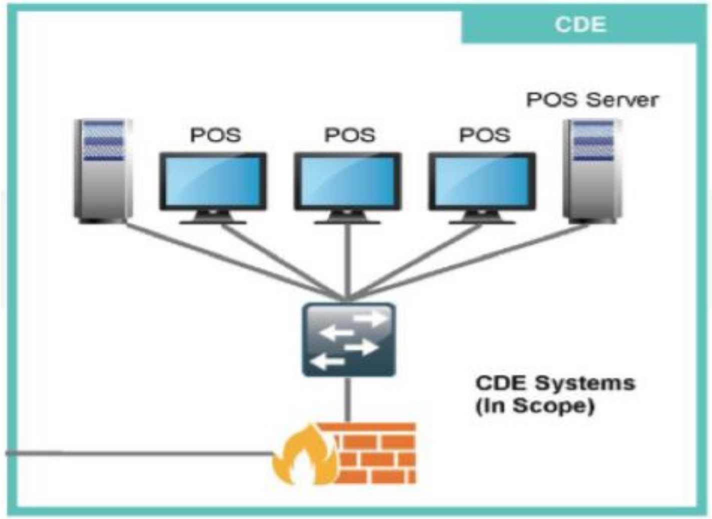
Defined Approach Requirements
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are:

Defined Approach Requirements
10.1.1 All security policies and operational procedures that are identified in Requirement 10 are:

Defined Approach Requirements
11.1.1 All security policies and operational procedures that are identified in Requirement 11 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.

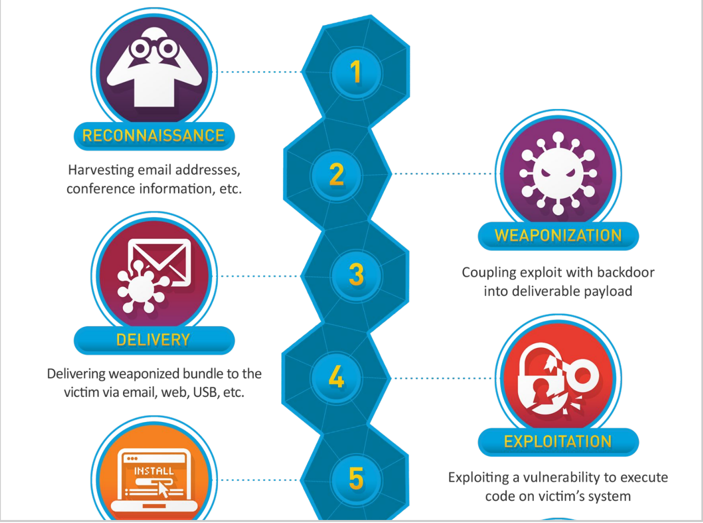
PCI DSS v4.0.1 Compliance in 3 Phases

Scope & Responsibility



Identify your store formats, define the CDE and connected-to systems, verify third-party responsibilities

Security Controls


RECONNAISSANCE
Harvesting email addresses, conference information, etc.
1
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
3
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL

Conduct your TRA, implement endpoint security, continuous monitoring, and authenticated vulnerability scanning

Policies & Procedures

Develop security awareness, incident response playbooks, and information security policies

Reach out - we're here to help.

Casey Brant

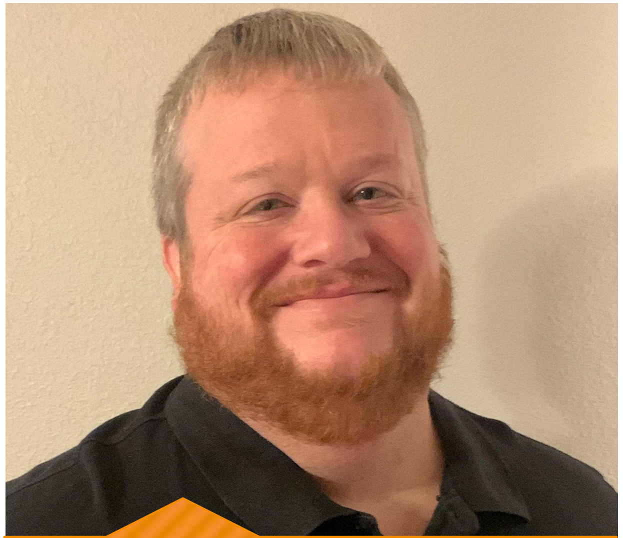
Standards Coordinator
Conexxus, Inc.
365@conexxus.org

Phil Stead

VP of Sales
Acumera, Inc
phil.stead@acumera.com

Ashwin Swamy

CEO
Omega ATC
ashwin.swamy@omegaatc.com
636-557-6000



Gregory DeClue

Cyber Operations Manager
Omega ATC
greg.declue@omegaatc.com
636-557-6000

Stay Tuned for

Q&A