



PCI DSS version 4.0 Overview

Reviewing the changes to the DSS

Presented by:

Viviana Wesley, CISM, PCI QSA, ISO 27001 Auditor

About the Presenter

Viviana Wesley

- Principal Consultant with HALOCK Security Labs
- CISM, PCI QSA, ISO 27001 Auditor
- HALOCK's PCI DSS Subject Matter Expert and Solution Architect
- Serves as an expert witness for State Offices of Attorney General and Multidistrict litigation matters
- 23+ years of practical experience within Information Technology
- 13+ years specializing in Information Security
- University of Northern Iowa – Bachelor of Arts in Computer Science

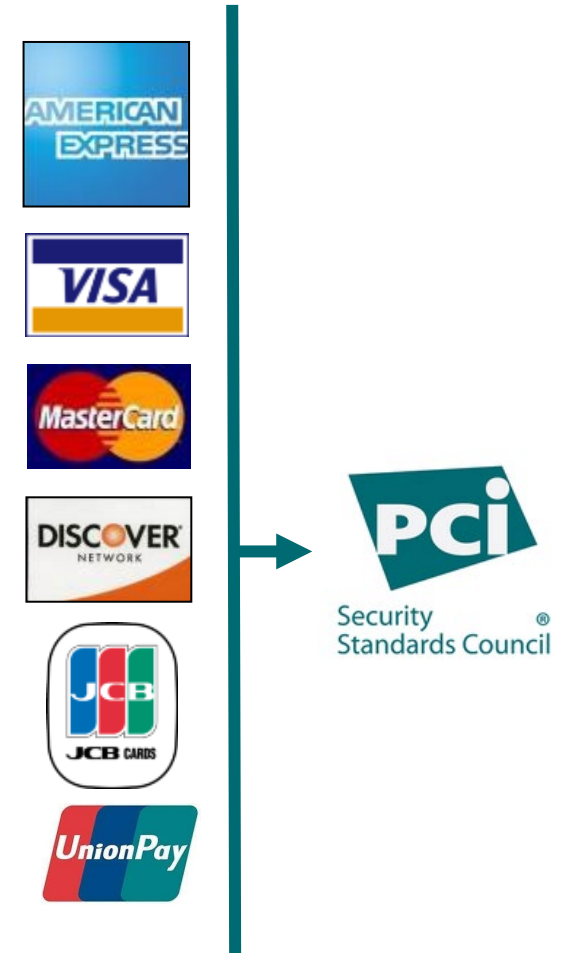


Agenda

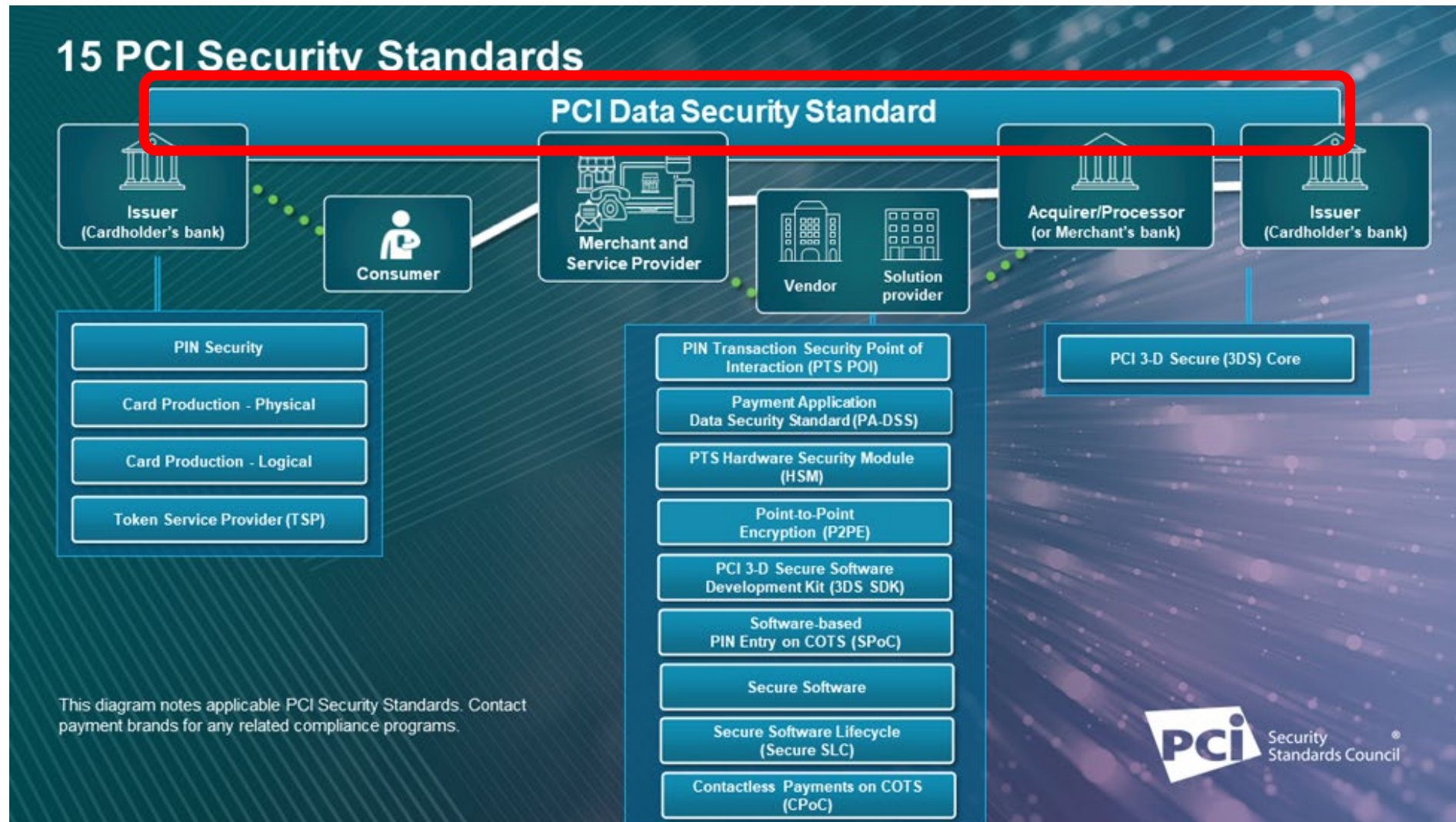
- Introduction
- What's Changed in PCI DSS 4.0
- Version 4.0 Requirement Changes
- Reporting Changes

What is PCI SSC?

- **Payment Card Industry Security Standards Council (SSC)**
- The SSC is an independent industry standards body providing oversight of the development and management of Payment Card Industry Security Standards on a global basis
- Founding multi-national acceptance brand members:
 - Visa, Inc.
 - MasterCard Worldwide
 - American Express
 - Discover Financial
 - JCB
 - **UnionPay (added September 2022)**



Overview of the PCI Standards



Source: <https://www.pcisecuritystandards.org/standards/>

What is the PCI DSS?

- **PCI DSS** = Payment Card Industry Data Security Standard
- Collaboration of payment brands
 - 1st version was published in December 2004
 - Version 3.2.1 became effective January 2019
 - 4.0 was published in March of 2022
 - **3.2.1 will be retired in March of 2024**
 - **51 New 4.0 requirements are best practices until March of 2025**
- Objective
 - Security
 - 'Low' bar
- Does it apply to me?
- POS, mail, IVR (Interactive Voice Response), e-commerce, and offline processes

Merchants and Service Providers



Merchants

For the purposes of the PCI DSS, a **merchant** is defined as **any entity that accepts payment cards bearing the logos of any PCI SSC Participating Payment Brand as payment for goods and/or services.**

A merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.



Service Providers

A **service provider** is a business entity that is not a payment brand, **directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity.** This includes payment gateways, payment service providers (PSPs), and independent sales organizations (ISOs). **This also includes companies that provide services that control or could impact the security of cardholder data.** Examples include managed service providers that provide managed firewalls, IDS, and other services as well as hosting providers and other entities.

If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).

Impact of Non-Compliance

A non-compliant, compromised business could expect the following:

Damage to the organization's brand equity and reputation (lost business)

Forensic investigation costs (required by card brands)

Remediation costs

Business disruption

Possible loss of credit card processing privileges

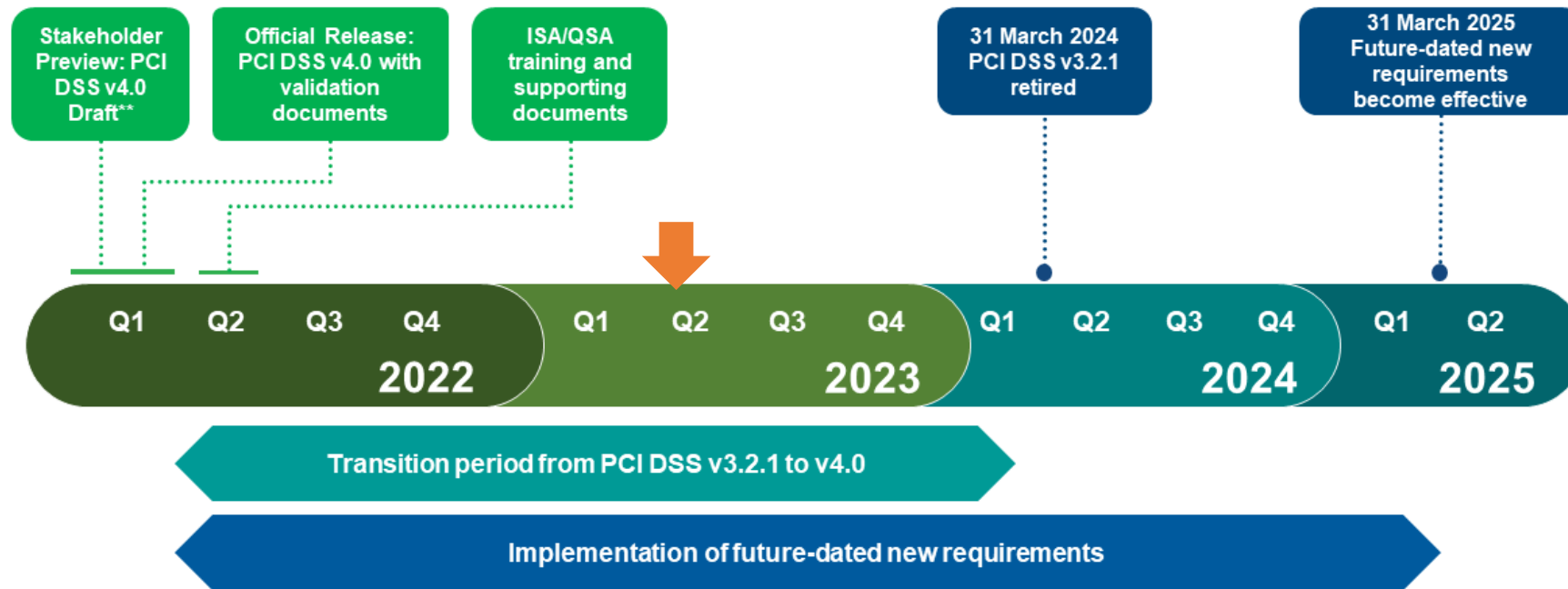
Possibility of business closure

Fines and Penalties

- Each brand issues separate fines, up to \$500,000 per incident
- Card re-issuance costs (avg. \$35 – \$40 per card)
- Chargebacks for fraudulent transactions
- Victim notification costs
- Even for small organizations, a single breach can easily cost \$10,000 to \$50,000

PCI DSS Transition Timeline

PCI DSS v4.0 Implementation Timeline*



* All dates based on current projections and subject to change

** Preview available to Participating Organizations, QSAs, and ASVs

Source: <https://blog.pcisecuritystandards.org/countdown-to-pci-dss-v4.0>

Summary of Changes in DSS 4.0

Change Types



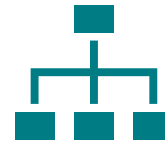
Evolving Requirement

- New requirements
- Updated requirements or testing procedures
- Deleted requirements



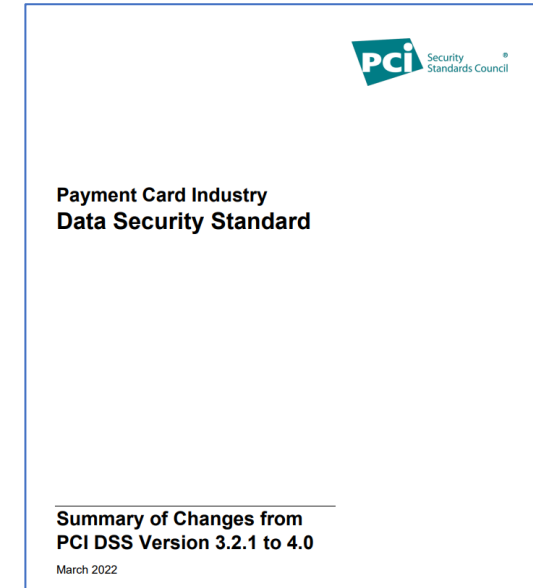
Clarification or Guidance

- Agreement between requirements and testing procedures
- Clearer language and Applicability Notes
- New appendices D and E



Structure or Format

- Combining and renumbering requirements



The overview section of each of the PCI DSS Requirement sections has been updated for guidance about scope and applicability.

A lot of extra guidance was added to the beginning of the DSS and in the Appendices.

Introducing the Customized Approach



New in PCI DSS 4.0

Defined Approach	Customized Approach
Same as PCI DSS v3.2.1	Flexibility for the entity
Defined Approach Testing Procedures	Extra documentation and risk analysis
Compensating Controls	No Compensating Controls

Steps for Using the Customized Approach: Appendix D in DSS 4.0 for more information

Assessed Entity	QSA Assessor
<ul style="list-style-type: none"> - Document and maintain evidence about each customized control - Perform targeted risk analysis - Test and monitor the control 	<ul style="list-style-type: none"> - Review entities evidence (targeted risk analysis and controls matrix) - Develop custom testing procedure - Test the control

PCI DSS Targeted Risk Analysis



Understanding Mischief

Mischief in PCI DSS 4.0 refers to an occurrence or event that negatively affects the security posture of the entity.

Objective:	Mischief:
Malicious software <i>cannot</i> execute	Malicious software executes
Daily responsibilities for activates <i>are</i> allocated	Responsibilities are <i>not</i> allocated

Completing the Targeted Risk Analysis (TRA) Template:

Part 1: Identify the requirement

Including the '**mischief**' it was designed to prevent

Part 2: Describe the proposed solution

Including how it will prevent the **mischief**

Part 3: Analyze changes to LIKELIHOOD of a breach

Including if likelihood of **mischief** occurring has changed

Part 4: Analyze changes to IMPACT of unauthorized access to account data

The amount of PAN data that can affected

Part 5: Approval and Review

Executive management

PCI Secure Software Framework & 4.0

The PA-DSS was retired in October of 2022 and replaced with the **PCI Software Security Framework**

The PCI Software Security Framework contains **two standards**:

1. Secure Software Lifecycle (Secure SDLC) Standard

Secure SLC assessors perform assessments of **software development processes** and Secure Software Assessors perform assessments of **software**.

2. Secure Software Standard

Software that is developed and maintained in accordance with either standard **can help the entity to meet several requirements in *PCI DSS Requirement 6* without having to perform additional detailed testing.**

Requirement 6 contains 3 sub-requirements that may be affected if an entity uses validated software:

- **6.2** Bespoke and custom software is developed securely.
- **6.3** Security vulnerabilities are identified and addressed.
- **6.5** Changes to all system components are managed securely.

Version 4.0 PCI DSS Requirements Overview



Total of 64 new PCI DSS Requirements

- 53 of which are applicable to all entities
- 11 of which are only applicable to Service Providers
- 13 of which are effective immediately for all version 4.0 validations
- 51 of which are effective on March 31st, 2025

Most existing PCI DSS requirements were impacted (updated, moved or removed) as part of this version release.

New Roles & Responsibilities requirement for sections 1 through 11.
This makes up 11 of the 13 new effective immediately requirements.

Overview of Changes to Requirement 1

Network Security Controls (NSC)



Network Security Controls (NSC) may include

- Physical firewalls
- Virtual devices
- Cloud access controls
- Virtualization or container systems
- Software-defined networking technology

Changes include:

- **1.1.2** - Roles and Responsibilities.
- **1.2.2** - Changes to **configurations of NSCs must be done in accordance with requirement 6** – which covers change management.
- **1.2.7** - Configurations of NSCs are reviewed every six months – **not just firewall rule sets, but all the controls relevant to requirement 1.**
- **1.2.8** - Configuration files for NSCs are secured and kept consistent with active configurations. **This replaces the old language of ‘secure and synchronized’ which only applied to routers.**
- Term “firewalls and routers” replaced with “NSC”.

Overview of Changes to Requirement 2

Apply Secure Configurations to All System Components



Changes include:

- **2.1.2** - Roles and Responsibilities.
- Updated title focuses on secure configurations in general, and **not just on vendor-supplied defaults**.
- **2.2** - Configuration standards **must now account for new vulnerabilities** that are identified (defined in requirement 6).
- **2.3.2** - If there are **multiple primary functions**, they can either be isolated or secured to the level required by the function with the highest security need.



Note:

The requirement for an inventory of system components has moved from requirement 2 into requirement 12.

Overview of Changes to Requirement 3

Protect Stored Account Data

FAQ 1091: Acceptable PAN Truncation Formats

Excluding the annexes, there are **7 requirements that are not eligible for the customized approach**, and **6 of them are found within Requirement 3 of the DSS** (the 7th is ASV scanning).

PAN / BIN Length	Payment Brand	Acceptable PAN Truncation Formats
16-digit PAN (with either 6- or 8-digit BIN)	Discover JCB Mastercard UnionPay Visa	At least 4 digits removed. Maximum digits which may be retained: "First 8, any other 4"
15-digit PAN	American Express	At least 5 digits removed. Maximum digits which may be retained: "First 6, last 4"
<15-digit PAN	Discover	Maximum digits which may be retained: "First 6, any other 4"

Changes include:

- **3.1.2** - Roles and Responsibilities.
- **3.2.1 & 3.3.2** - Coverage for SAD stored pre-authorization and encryption.
- **3.5.1.1** – Hashing used to render PAN unreadable must be keyed cryptographic hashes.
- **3.4.2** - Technical control must prevent moving or copying of CHD via remote access technology.
- **3.5.1.2** - Disk encryption not sufficient for non-removable media.
- **3.6.1.1** - Service Providers cannot use the same encryption keys in prod/test environments.
- Masking and truncating rules.
 - Masking is now 'no more than BIN and last 4 digits'
 - Truncating is governed by FAQ 1091

March
2025



Overview of Changes to Requirement 4

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



Changes include:

- **4.1.2 – Roles and Responsibilities**
 - Documented, assigned and understood.
- **4.2.1 – Valid Certificates**
 - Must be trusted, issued from a trusted source, not expired.
- **4.2.1.1 – Inventory of trusted keys and certificates**
 - Used to protect PAN during transmission.



Note:

4.2.1 also provides guidance around receiving CHD that is not expected and the use of self-signed certificates in the new Applicability Notes.

March
2025

Overview of Changes to Requirement 5

Protect All Systems and Networks from Malicious Software

Changes include:

- 5.1.2 - Roles and Responsibilities.
- 5.2.3.1 & 5.3.2.1 - Frequencies based on Targeted Risk Analysis (for at not-at-risk components and scan frequency).

March
2025

- 5.3.2 - Option for continuous behavioral analysis.

- 5.3.3 - Anti-malware for Removable Electronic media.
- 5.4.1 - Anti-phishing mechanism.

March
2025



- Term “Anti-virus” replaced with “Anti-malware”.
- Term “Not Commonly Affected” replaced with “Not at risk”.



Overview of Changes to Requirement 6

Develop and Maintain Secure Systems and Software



Changes include:

- **6.1.2** - Roles and Responsibilities.
- **6.3.2** - Bespoke and custom software inventory.
- **6.4.2** - WAF will be required, 6.6 penetration testing retired.
- **6.4.3** - Payment page scripts are authorized, managed and inventoried.



March
2025

- Reorganization of requirements.
- Separation of roles (clarification update).
- Live PANs for testing (allowed when pre-production is in scope).
- Term “development and test” replaced with “pre-production”.



Overview of Changes to Requirement 7

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

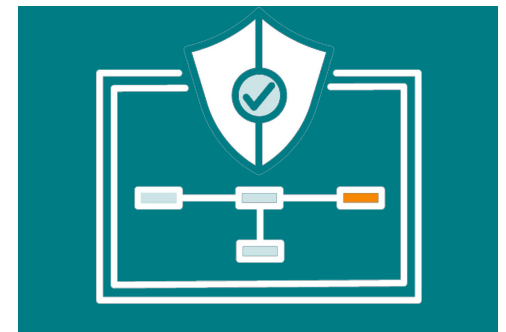
Changes include:

- **7.1.2** - Roles and Responsibilities.
- **7.2.4** - User account/privilege review every 6 months.
- **7.2.5** - Application and system accounts management.
- **7.2.5.1** - Application and system accounts review periodically.

March
2025

- **Clarified scope of requirements**

- Apply to user accounts and access for employees, contractors, consultants, and internal and external vendors and other third parties.
- Requirements do not apply to consumer accounts.



Overview of Changes to Requirement 8

Identify Users and Authenticate Access to System Components



Changes include:

- **8.1.2** - Roles and Responsibilities.
- **8.3.6** - Password length increase (12 if supported or 8).
- **8.3.10.1** - Service Providers with non-consumer customer accounts, 90-day expiration or zero trust.
- **8.4.2** - MFA for all access into the CDE.
- **8.5.1** - MFA implementation protections.
- **8.6.1** - System/Application accounts with interactive logins are managed.
- **8.6.2** - No hard-coded passwords for System/Application accounts.
- **8.6.3** - Management of system/application account passwords



March
2025



Overview of Changes to Requirement 9

Restrict Physical Access to Cardholder Data

Changes include:

- **9.1.2** - Roles and Responsibilities.
- **9.5.1.2.1** – Periodic inspections of POI devices based on TRA.

March
2025

- Overview of requirement 9 was updated to give guidance about areas that are in-scope. Each relevant requirement now states one of three areas, the CDE, sensitive areas or the facility.
- **Sensitive area** defined in the glossary (now a DSS appendix).
- Facility defined in the overview section.



Overview of Changes to Requirement 10

Log and Monitor All Access to System Components and Cardholder Data

Changes include:

- **10.1.2** - Roles and Responsibilities.
- **10.4.1.1** - Automated mechanisms are used to perform audit log reviews.
- **10.4.2.1** - Log Review Period defined by TRA.
- **10.7.2** - Detect and alert on failures of critical security controls (currently only applies to Service Providers).
- **10.7.3** - Respond promptly to critical security control failures.



March
2025



Overview of Changes to Requirement 11

Test Security of Systems and Network Regularly

Changes include:

- 11.1.2 - Roles and Responsibilities.
- 11.3.1.1 - All other vulnerabilities addressed based on TRA.
- 11.3.1.2 - Internal authenticated scanning. 
- 11.4.7 - Multi-tenant service providers support their customers external penetration testing needs.
- 11.5.1.1 - Service Providers: IDS/IPS or other to alert/prevent and address covert malware communication channels.
- 11.6.1 - Detect and report changes to payment pages. 

March
2025




Overview of Changes to Requirement 12

Support Information Security with Organizational Policies and Programs




Changes include:

March 2025

- **12.3.1** - Targeted Risk Analysis (periodic cadence requirements).
- **12.3.3** - Cryptographic agility.
- **12.3.4** - Hardware and software review. 
- **12.3.2** – Targeted Risk Analysis for Customized Approach requirements.
- **12.5.2** - Document and confirm scope.



March 2025

- **12.5.2.1** - Service Providers: Document and confirm scope bi-annually.
- **12.5.3** - Service Providers: significant change to organization structure, requires additional scope review.
- **12.6.2** - Security awareness training reviewed and updated annually. 
- **12.6.3.1** - Training includes awareness of threats (phishing, social engineering, etc.).
- **12.6.3.2** - Training includes acceptable use for end-user technologies.

March 2025

- **12.9.2** - Service Provider: Support their customer’s request for PCI compliance status and responsibilities.
- **12.10.4.1** - Frequency of periodic incident response training is based on TRA.
- **12.10.5** - Inclusion of alerts from payment page tampering.
- **12.10.7** - Unexpected PAN incident response procedures.

Overview of Changes to Appendix A1

Multi-Tenant Service Providers

Changes include:

- **A1.1.1** - Logical separation between provider and customers
- **A1.1.4** - Confirm logical controls between customers
- **A1.2.3** - Reporting and addressing suspected or confirmed incidents



Overview of Changes to Reporting

Changes include:

- **ROC and AOC** sections now align.
- **SAQ and AOC** sections now align.
- **SAQs** now use the DSS requirements.
- **New section** for Remote Assessments.
- **ROC template expanded executive summary sections** for more detail, more ways to track documentation, evidence, samples, interviews and observations.
- **ROC template has reduced write-ups** (typically 1 per requirement) all other references comes from the executive summary.
- **No new SAQ Types.**
- SAQs now include **expanded** executive summary sections.
- **Service Providers will have to complete write-ups** in their SAQ type D.
- **No Customized Approach for the SAQs.**



Other Updates

New 4.0 documents were published in Q1 2023.

- Removed the In-Place with Remediation status – for now.

4.0 Transition Training available to QSAs.

- Been released to QSAs, with lighter versions available to ISAs and PCIPs.

Re-qualification Training will be against version 4.0 in 2024.

SAQ clients that validate compliance through a portal may need to move to 4.0 before March 2024 – this will be dependent on portal's transition timing.

Clients outsourcing to third party service providers, may need information from that third party in order to determine applicability to them for new requirements.



Questions?

Viviana Wesley, CISM, PCI QSA, ISO 27001 Auditor vwesley@halock.com

<https://www.halock.com>

[PCI Compliance articles](#)