Tevora White Paper, August 2024

TEVORA™ | White Paper

Countdown to PCI DSS v4.0 Compliance:

WHAT IS THE MOST SIGNIFICANT IMPACT?

This Paper identifies the most significant impacts you can expect to face in complying with PCI DSS version 4.0. We'll cover PCI DSS v4.0 goals, types of changes being introduced, implementation timeline, potentially significant budget impacts, and requirements that are likely to require the most time to implement.

What's Changing with PCI DSS v4.0?

When developing PCI DSS v4.0, the PCI Security Standards Council had four goals. These are listed below, along with examples of changes being implemented to address each goal[1].

PCI DSS 4.0 Goals and Change Examples

Goal	Why It's Important	Examples
1. Continue to meet the security needs of the payments industry.	Security practices must evolve as threats change.	▶ Expanded multi-factor authentication requirements. ▶ Updated password requirements. ▶ New e-commerce and phishing requirements to address ongoing threats.
2. Promote security as a continuous process.	Criminals never sleep. Ongoing security is crucial to protect payment data.	▶ Clearly assigned roles and responsibilities for each requirement. ▶ Added guidance to help people better understand how to implement and maintain security.
3. Increase flexibility for organizations using different methods to achieve security objectives.	Increased flexibility allows more options to achieve a requirement's objective and supports payment technology innovation.	▶ Allowance of group, shared, and generic accounts. ▶ Targeted risk analyses empower organizations to establish frequencies for performing certain activities. ▶ Customized Approach, a new method to implement and validate PCI DSS requirements, provides another option for organizations using innovative methods to achieve security objectives.
4. Enhance validation methods and procedures.	Clear validation and reporting options support transparency and granularity.	▶ Increased alignment between information reported in a Report on Compliance or Self-Assessment Questionnaire and information summarized in an Attestation of Compliance.

[1] PCI DSS 4.0 At a Glance, v4.0, December 2022

Change Types

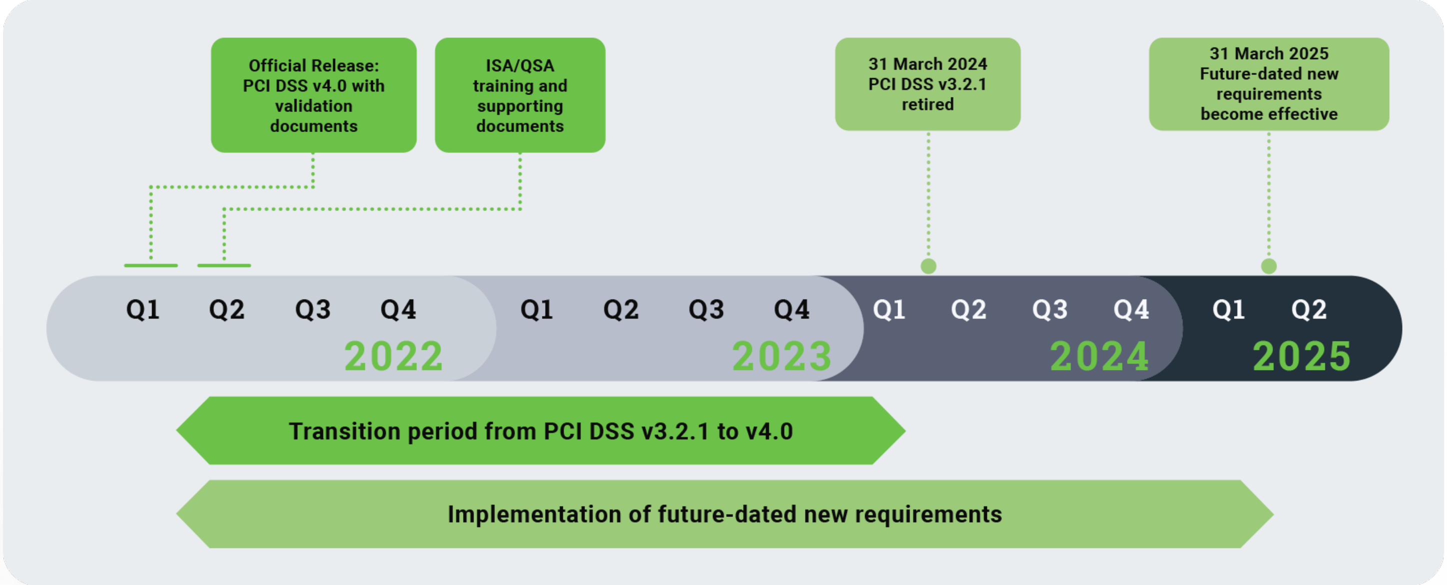
PCI DSS 4.0 includes three types of changes[2]:

- Evolving Requirements: Changes to ensure that the standard is up to date with emerging threats and technologies, and changes in the payment industry. Examples include new or modified requirements or testing procedures, or the removal of a requirement.
- Clarification or Guidance: Updates to wording, explanation, definition, additional guidance, and/or instruction to increase understanding or provide further information or guidance on a particular topic.
- Structure or Format: Reorganization of content, including combining, separating, and renumbering of requirements to align content.

Implementation Timeline

The planned timeline for implementation of PCI DSS v4.0 is summarized below. PCI v4.0 was published in 2022, with the prior version (PCI DSS v3.2.1) remaining in place until it was retired March 31, 2024. Some v4.0 requirements are future-dated and do not become effective until March 31, 2025. This provides organizations time to become familiar with the new version and plan for and implement the needed changes.

PCI DSS v4.0 Implementation Timeline[3]


Official Release: PCI DSS v4.0 with validation documents
ISA/QSA training and supporting documents
31 March 2024 PCI DSS v3.2.1 retired
31 March 2025 Future-dated new requirements become effective
Q1 Q2 Q3 Q4 2022
Q1 Q2 Q3 Q4 2023
Q1 Q2 Q3 Q4 2024
Q1 Q2 2025
Transition period from PCI DSS v3.2.1 to v4.0
Implementation of future-dated new requirements

Start Your Planning Budget Now

Some of the PCI DSS v4.0 changes may have significant budget impacts (e.g., purchasing new security solutions or tools). If you haven't started already, we recommend that you begin your budget planning for these changes as soon as possible.

Tevora's team of PCI DSS and cybersecurity experts has identified the PCI DSS v4.0 requirements that are likely to have the greatest budget impacts on your organization. The table below summarizes these requirements.

[2] Summary of Changes from PCI DSS Version 3.2.1 to 4.0, Revision 2, December 2022

[3] PCI DSS 4.0 At a Glance, v4.0, December 2022

PCI DSS v4.0 Requirements with Potentially Significant Budget Impacts

PCI DSS v3.2.1	PCI DSS v4.0	Description of Change	Change Type
2.3.10	3.4.2	**New requirement** for technical controls to prevent copy and/or relocation of PAN when using remote-access technologies. Expanded from former Requirement 12.3.10. *This requirement is a best practice until 31 March 2025.*	Evolving Requirement
	5.3.3	**New Requirement** for a malware solution for removable electronic media. *This requirement is a best practice until 31 March 2025.*	Evolving Requirement
	5.4.1	**New requirement** to detect and protect personnel against phishing attacks. *This requirement is a best practice until 31 March 2025.*	Evolving Requirement
	6.4.2	**New requirement** to deploy an automated technical solution for public-facing web applications that continually detects and prevents web-based attacks. This new requirement removes the option in Requirement 6.4.1 to review web applications via manual or automated application vulnerability assessment tools or methods. *This requirement is a best practice until 31 March 2025.*	Evolving Requirement
	6.4.3	**New requirement** for management of all payment page scripts that are loaded and executed in the consumer's browser. *This requirement is a best practice until 31 March 2025.*	Evolving Requirement
	8.4.2	**New requirement** to implement multi-factor authentication (MFA) for all access into the CDE. *This requirement is a best practice until 31 March 2025.* Added a note to clarify that MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3; and that applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access.	Evolving Requirement
	8.5.1	**New requirement** for secure implementation of multi-factor authentication systems. *This requirement is a best practice until 31 March 2025.*	Evolving Requirement
	8.6.1	**New requirement** for management of system or application accounts that can be used for interactive login. *This requirement is a best practice until 31 March 2025.*	Evolving Requirement
	10.4.1.1	**New requirement** for the use of automated mechanisms to perform audit log reviews. *This requirement is a best practice until 31 March 2025.*	Evolving Requirement

PCI DSS v4.0 Requirements with Potentially Significant Budget Impacts (cont.)

PCI DSS v3.2.1	PCI DSS v4.0	Description of Change	Change Type
	10.7.2	**New requirement** for all entities to detect, alert, and promptly address failures of critical security control systems. *This requirement is a best practice until 31 March 2025.* This new requirement applies to all entities – it includes two additional critical security controls not included in Requirement 10.7.1 for service providers.	Evolving Requirement
	11.3.1.2	**New Requirement** to perform internal vulnerability scans via authenticated scanning. *This requirement is a best practice until 31 March 2025.*	Evolving Requirement
11.3	11.4.1	Clarified the following: ▶ The methodology is defined, documented, and implemented by the entity. ▶ Penetration testing results are retained for at least 12 months. ▶ The methodology includes a documented approach to assessing and addressing risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. ▶ The meaning of testing from inside the network (internal penetration testing) and from outside the network (external penetration testing).	Clarification or Guidance
	11.5.1.1	**New requirement for service providers** to use intrusion-detection and or intrusion-prevention techniques to detect, alert on/prevent, and address covert malware communication channels. *This requirement is a best practice until 31 March 2025.*	Evolving Requirement
	11.6.1	**New requirement** to deploy a change-and-tamper-detection mechanism to alert for unauthorized modifications to the HTTP headers and contents of payment pages as received by the consumer browser. *This requirement is a best practice until 31 March 2025.*	Evolving Requirement
	12.6.3.1	**New requirement** for security awareness training to include awareness of threats and vulnerabilities that could impact the security of the CDE. *This requirement is a best practice until 31 March 2025.*	Evolving Requirement
	12.6.3.2	**New requirement** for security awareness training to include awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1. *This requirement is a best practice until 31 March 2025.*	Evolving Requirement

Requirements Likely to Have Long Implementation Timeframes

Many of the PCI DSS v4.0 requirements are likely to take a significant amount of time for your organization to implement. In this section, we summarize the requirements that Tevora's experts believe will take the most time to implement. We recommend that your implementation plan be designed to begin work on these requirements as early as possible

Document Roles and Responsibilities for New or Updated PCI DSS v4.0 Requirements

Organizational roles and responsibilities must be updated to reflect the following PCI DSS v4.0 requirements:

- Requirement 2.1.2: Updated principal requirement title to reflect that the focus is on secure configuration in general, and not just on vendor supplied defaults.
- Requirement 3.1.2: Updated principal requirement title to reflect the focus on account data.
- Requirement 4.1.2: Updated principal requirement title to reflect the focus on "strong cryptography" to protect transmissions of cardholder data.
- Requirement 5.1.2: Updated principal requirement title to reflect the focus on protecting all systems and software. Replaced "anti-virus" with "anti-malware" throughout to support a broader range of technologies used to meet the security objectives traditionally met by anti-virus software.
- Requirement 6.1.2: Updated principal requirement title to include "software" rather than "applications." Clarified that Requirement 6 applies to all system components, except for Requirement 6.2, which applies only to bespoke and custom software.
- Requirement 7.1.2: Updated principal requirements title to include system components and cardholder data.
- Requirement 8.1.2: Standardized on terms "authentication factor" and "authentication credentials." Removed "non-consumer users" and clarified in the overview that requirements do not apply to accounts used by consumers (cardholders). Removed note in overview that listed requirements that do not apply to user accounts with access to only one card number at a time to facilitate a single transaction and added that note to each related requirement.
- Requirement 9.1.2: In the overview, clarified the three different areas covered in Requirement 9 (sensitive areas, CES, and facilities). Throughout, clarified whether each requirement applies to the CDE, sensitive areas, or facilities.
- Requirement 10.1.2: Updated principal requirements title to reflect focus on audit logs, system components, and cardholder data. Clarified that these requirements do not apply to user activity of consumers (cardholders). Replaced "Audit trails" with "Audit logs" throughout.
- Requirement 11.1.2: Minor update to principal requirement title.
- Requirement 11.6.1: New requirement to deploy a change-and-tamper-detection mechanism to alert for unauthorized modifications to the HTTP headers and contents of payment pages as received by the consumer browser.

New/Updated PCI DSS v4.0 Requirements Related to Targeted Risk Analysis

PCI DSS v4.0 removes the requirement for a formal organization-wide risk assessment and replaces it with requirements for specific targeted risk analyses. Below is a summary of specific requirements related to targeted risk analysis as well as corresponding requirements that should be taken into account when performing targeted risk analyses

- Requirement 12.3.1: New requirement to perform a targeted risk analysis for any new PCI DSS requirement that provides flexibility for how frequently it is performed.
- Requirement 12.3.2: New requirement for entities using a Customized Approach to perform a targeted risk analysis for each PCI DSS requirement that the entity meets with the customized approach.
- Requirement 5.2.3.1: New requirement to define the frequency of periodic evaluations of system components not at risk for malware in the entity's targeted risk analysis.
- Requirement 5.3.2.1: New requirement to define the frequency of periodic malware scans in the entity's targeted risk analysis.
- Requirement 7.2.5.1: New requirement for the review of all access by application and system accounts and related access privileges.
- Requirement 8.6.3. New requirement for protecting passwords/passphrases for application and system accounts against misuse.
- Requirement 9.5.1.2.1. New requirement to define the frequency of periodic Point of Interaction (POI) device inspections based on the entity's targeted risk analysis.
- Requirement 10.4.1. The following audit logs are reviewed at least once daily:
    - All security events.
    - Logs of all system components that store, process, or transmit CHD and/or SAD.
    - Logs of all critical system components.
    - Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).
- Requirement 11.3.1.1. New requirement to manage all other applicable vulnerabilities (those not ranked as high-risk or critical) found during internal vulnerability scans.
- Requirement 12.10.4.1. New requirement to perform targeted risk analysis to define the frequency of periodic training for incident response personnel.

Other PCI DSS v4.0 Requirements with Long Implementation Timeframes

- Requirement 6.3.1. Added a bullet to clarify applicability to vulnerabilities for bespoke and custom and third-party software.
- Requirement 6.3.2. New requirement to maintain an inventory of bespoke and custom software.
- Requirement 11.6.1. New requirement to deploy a change-and-tamper-detection mechanism to alert for unauthorized modifications to the HTTP headers and contents of payment pages as received by the consumer browser.
- Requirement 8.6.2. New requirement for not hard-coding passwords/passphrases into files or scripts for any application and system accounts that can be used for interactive login.
- Requirement 12.3.3. New requirement to document and review cryptographic cipher suites and protocols in use at least once every 12 months.
- Requirement 12.3.4. New requirement to review hardware and software technologies in use at least once every 12 months.
- Requirement 12.5.2. New requirement to document and confirm PCI DSS scope at least every 12 months and upon significant change to the in-scope environment.
- Requirement 12.5.2.1. New requirement for service providers to document and confirm PCI DSS scope at least once every six months and upon significant change to the in-scope environment.

Additional Resources

Below are additional resources that provide a deeper dive into the topics covered in this white paper:

- PCI DSS v4.0 At a Glance
- PCI DSS Summary of Changes from v3.2.1 to v4.0 – December 2022
- PCI DSS Requirements and Testing Procedures, Version 4.0, March 2022
- Tevora Webinar: Deciphering PCI DSS v4.0: How to Prepare your Organization
- Tevora Blog Post: PCI DSS Launches Version 4.0

We can help.

Tevora is your **comprehensive cybersecurity resource.**

As an experienced Payment Card Industry Qualified Assessor, Tevora's team of experts can answer any questions you have about PCI DSS v4.0. We would also welcome the opportunity help your organization plan for and implement the changes needed to comply with this significant PCI DSS release. Just give us a call at **(833) 292-1609** or email us at **sales@tevora.com**.

TEVORA™

Go forward. **We've got your back.**