



Payment Card Industry ● Data Security Standard

Summary of Changes from PCI DSS Version 3.2.1 to 4.0

March 2022 ●

Table of Contents

1	Introduction.....	1
● 2	Change Types	2
3	Summary of Changes to PCI DSS Introductory Sections	2
4	Summary of General Changes to PCI DSS Requirements	5
5	Additional Changes per Requirement	6
● 6	Summary of New Requirements	29

1 Introduction

This document provides a high-level summary and description of the changes from PCI DSS v3.2.1 to PCI DSS v4.0 and does not detail all document revisions. Due to the extent of the changes, the standard should be reviewed in its entirety rather than focusing solely on this summary document.

This Summary of Changes is organized as follows:

- *Change Types* - provides an overview of the types of changes
- *Summary of Changes to PCI DSS Introductory Sections* - summarizes changes made for each affected section.
- *Summary of General Changes to PCI DSS Requirements* - summarizes changes made throughout the requirements, testing procedures, and guidance.
- *Additional Changes per Requirement* - summarizes additional changes made in requirements 1-12 and the appendices.
- *Summary of New Requirements* - lists all new requirements, the entity to which the new requirement applies (that is, all entities or service providers only), and the effective date of the new requirement.

2 Change Types

Change Type	Definition
● Evolving requirement	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.

3 Summary of Changes to PCI DSS Introductory Sections

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Introduction and PCI Data Security Standard Overview	Introduction and PCI Data Security Standard Overview	Added "Limitations" sub-heading and clarified that PCI DSS does not supersede county, state, or local laws. Expanded list of PCI DSS resources.	Clarification or guidance
PCI DSS Applicability Information	PCI DSS Applicability Information	Added sub-headings to increase readability. Clarified that some PCI DSS requirements may apply for entities that do not store, process, or transmit primary account number (PAN). Clarified that terms account data, sensitive authentication data (SAD), cardholder data, and PAN are not interchangeable and are used intentionally in PCI DSS. Clarified table with commonly used elements of cardholder data and SAD, whether storage is permitted, and whether data must be rendered unreadable.	Clarification or guidance
Relationship between PCI DSS and PA-DSS	Relationship between PCI DSS and PCI SSC Software Standards	Refocused section on relationship between PCI DSS and PCI SSC software standards, with mention of PA-DSS (retiring in October 2022).	Evolving requirement
Scope of PCI DSS Requirements	Scope of PCI DSS Requirements	Clarified applicability of PCI DSS requirements and the definition of cardholder data environment (CDE). Expanded examples of system components to which PCI DSS applies; added cloud and other system components. Added "Understanding PCI DSS Scoping" diagram.	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Scope of PCI DSS Requirements	Scope of PCI DSS Requirements: Annual PCI DSS Scope Confirmation	Added sub-heading and clarified existing content.	Clarification or guidance
Appendix D: Segmentation and Sampling of Business Facilities/System Components	Scope of PCI DSS Requirements: Segmentation	Moved segmentation diagram formerly in Appendix D, with minor edits. Retitled sub-section and updated references from 'network segmentation' to 'segmentation' to support a broader range of segmentation controls.	Clarification or guidance
Scope of PCI DSS Requirements: Wireless	Scope of PCI DSS Requirements: Wireless	Clarified that rogue wireless detection (Requirement 11.2.1) must be performed even if wireless is not used in the CDE and even if the entity has a policy that prohibits its use.	Clarification or guidance
	Scope of PCI DSS Requirements: Encrypted Cardholder Data and Impact on PCI DSS Scope	Added sub-section and related content.	Clarification or guidance
	Scope of PCI DSS Requirements: Encrypted Cardholder Data and Impact to PCI DSS Scope for Third-Party Service Providers	Added new sub-section and related content.	Clarification or guidance
Scope of PCI DSS Requirements: Use of Third-party Service Providers/Outsourcing	Scope of PCI DSS Requirements: Use of Third-party Service Providers	Retitled sub-section, added new content, and reorganized existing content under new sub-headings.	Clarification or guidance
● Best Practices for Implementing PCI DSS into Business-as-Usual Processes	Best Practices for Implementing PCI DSS into Business-as-Usual Processes	Added guidance and clarifications throughout.	Clarification or guidance
For Assessors: Sampling of Business Facilities/System Components	For Assessors: Sampling for PCI DSS Assessments	Retitled section and updated throughout with additional guidance and clarifications. Clarified that sampling references were removed from Testing Procedures to support assessors in selecting samples that are appropriate to the population being tested.	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
● Appendix D: Segmentation and Sampling of Business Facilities/System Components	For Assessors: Sampling for PCI DSS Assessments	Moved sampling diagram formerly in Appendix D, with minor edits.	Clarification or guidance
	Description of Timeframes Used in PCI DSS Requirements	New section to clarify frequencies and timeframes specified in PCI DSS and related expectations. Added explanation of “significant change.”	Clarification or guidance
	Approaches for Implementing and Validating PCI DSS	New section to explain and illustrate the two approaches, defined and customized, for implementing and validating PCI DSS.	Evolving requirement
● Compensating Controls	Approaches for Implementing and Validating PCI DSS	Moved content to this section, at a sub-heading under “Defined Approach.”	Structure or format
	Protecting Information About Entity’s Security Posture	New section to describe how entities may handle sensitive artifacts from their PCI DSS assessment.	Clarification or guidance
	Testing Methods for PCI DSS Requirements	New section to describe the testing methods used in each PCI DSS Testing Procedures and corresponding expected activities to be performed by the assessor.	Clarification or guidance
PCI DSS Assessment Process	PCI DSS Assessment Process	Includes minor clarifications. Moved note that starts “PCI DSS requirements are not considered to be in place...” here, formerly in Detailed PCI DSS Requirements and Security Assessment Procedures.	Clarification or guidance
	Additional References	New section that lists external organizations referenced within PCI DSS requirements or guidance.	Clarification or guidance
Detailed PCI DSS Requirements and Security Assessment Procedures	Detailed PCI DSS Requirements and Testing Procedures	Replaced content on first page of section with an illustration that explains all elements of the Requirements column, Testing Procedures column, and Guidance column. To first page of section, added description for Requirements noted with “Additional requirements for service providers only.” To first page of section, added summary of appendices that include additional PCI DSS requirements for different types of entities.	Clarification or guidance

4 Summary of General Changes to PCI DSS Requirements









General Changes Implemented Throughout PCI DSS Requirements	Change Type
Reformatted overview sections and added a summary of the sections to the beginning of each principal requirement.	Structure or format
Updated overview sections and added guidance at the start of each requirement section.	Clarification or guidance
Added numbered requirement description headings throughout each requirement to organize and describe the requirements that fall under it.	Structure or format
Renumbered requirements and testing procedures and reorganized requirements due to the addition of numbered requirement description headings.	Structure or format
Rephrased directive requirements to be objective.	Evolving requirement
Moved examples from requirements or testing procedures into the guidance column.	Structure or format
Removed references to sampling from testing procedures.	Clarification or guidance
Shortened testing procedures by clarifying testing is to be done “in accordance with all elements specified in this requirement” to minimize redundancy between requirements and testing procedures.	Clarification or guidance
Updated language in requirements and/or corresponding testing procedures for alignment and consistency.	Clarification or guidance
Enhanced testing procedures to clarify level of validation expected for each requirement.	Clarification or guidance
Reformatted requirements and testing procedures and made minor wording changes for readability – for example, content from paragraphs reformatted to bullet points.	Structure or format
Combined requirements that support the same intent and separated requirements that support different intents.	Structure or format
Separated complex requirements / testing procedures and removed redundant or overlapping testing procedures.	Structure or format
Moved required elements that were included only in testing procedures to requirements, to clarify the requirement and to facilitate shortening of the testing procedures.	Clarification or guidance
Moved and reworded policies and procedures requirements from the end to the beginning of each principal requirement.	Structure or format
Removed notes about SSL/Early TLS from the guidance columns for requirements that referenced those specific protocols.	Clarification or guidance
Changed “cardholder data” to “account data” as needed to align with usage and intent.	Clarification or guidance
Changed terminology used to refer to frequency throughout the requirements in accordance with Description of Timeframes Used in PCI DSS Requirements.	Clarification or guidance
Added titles and reorganized content of the guidance column to aid understanding and merge similar information.	Structure or format







5 Additional Changes per Requirement





Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Requirement 1			
Requirement 1- General		Updated principal requirement title to reflect the focus on “network security controls.” Replaced “firewalls” and “routers” with “network security controls” to support a broader range of technologies used to meet the security objectives traditionally met by firewalls.	Evolving requirement
1.1.5	1.1.2	Replaced requirement for “Description of groups, roles, and responsibilities for management of network components” with general requirement for roles and responsibilities for Requirement 1.	Evolving requirement
1.1	1.2.1	Refocused former “null” requirement (all content pointed to other requirements) on defining, implementing, and maintaining configuration standards for network security control rulesets.	Clarification or guidance
1.1.1	1.2.2	Clarified that changes are managed in accordance with the change control process defined at Requirement 6.5.1.	Clarification or guidance
1.1.4		Removed redundant requirement.	Clarification or guidance
1.1.6	1.2.5 1.2.6	Separated into two requirements to clarify intent of each.	Clarification or guidance
1.1.7	1.2.7	Clarified the intent of reviewing configurations of network security controls at least once every six months.	Clarification or guidance
1.2		Removed “null” requirement (all content pointed to other requirements).	Structure or format
1.2.2	1.2.8	Clarified the intent of securing configuration files.	Clarification or guidance
1.2.1 1.3.4	1.3.1 1.3.2	Separated Requirement 1.2.1. into two requirements to clarify intent of each. Removed redundant Requirement 1.3.4.	Clarification or guidance
1.2.3	1.3.3	Clarified the intent of implementing network security controls between wireless networks and the CDE.	Clarification or guidance
1.3	1.4.1	Refocused a former null requirement (all content pointed to other requirements). Clarified that the intent is to implement controls between trusted and untrusted networks.	Clarification or guidance




Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
1.3.1 1.3.2 1.3.5	1.4.2	Merged requirements to clarify that the intent is to restrict inbound traffic from untrusted networks.	Clarification or guidance
1.3.6	1.4.4	Clarified the intent is that system components storing cardholder data are not directly accessible from untrusted networks.	Clarification or guidance
1.4	1.5.1	Clarified that the intent is to implement security controls on any computing device that connects to both untrusted networks and the CDE.	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Requirement 2			
Requirement 2 - General		Updated principal requirement title to reflect that the focus is on secure configurations in general, and not just on vendor-supplied defaults.	Clarification or guidance
	2.1.2	New requirement for roles and responsibilities. This requirement is effective immediately for all v4.0 assessments	Evolving requirement
2.1	2.2.2	Clarified that the intent is to understand whether vendor default accounts are in use and to manage them accordingly.	Clarification or guidance
2.2.1	2.2.3	Clarified the intent of the requirement for managing primary functions that require different security levels.	Clarification or guidance
2.2.2 2.2.5	2.2.4	Combined requirements to align similar topics.	Structure or format
2.2.3	2.2.5	Clarified that the intent of the requirement is if any insecure services, protocols, or daemons are present.	Clarification or guidance
2.1.1	2.3.1 2.3.2	Split requirement for changing all wireless vendor defaults into two requirements to clarify the focus of each.	Clarification or guidance
2.4	12.5.1	Moved requirement to align related content.	Structure or format
2.6		Removed "null" requirement (all content pointed to other requirements).	Structure or format
Requirement 3			
Requirement 3 - General		Updated principal requirement title to reflect the focus on account data.	Clarification or guidance
	3.1.2	New requirement for roles and responsibilities. This requirement is effective immediately for all v4.0 assessments.	Evolving requirement
3.1	3.2.1	New requirement bullet to address SAD stored prior to completion of authorization through implementation of data retention and disposal policies, procedures, and processes. This bullet is a best practice until 31 March 2025.	Evolving requirement
	3.3.2	New requirement to encrypt SAD that is stored electronically prior to completion of authorization. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving requirement



Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
3.2.a 3.2.b	3.3.3	Added a requirement to address former testing procedures that any storage of SAD by issuers is limited to that which is needed for a legitimate issuing business need and is secured.	Clarification or guidance
3.3	3.4.1	Clarified that PAN is masked when displayed such that only personnel with a business need can see more than the BIN/last four digits of the PAN.	Evolving  requirement
12.3.10	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. <i>This requirement is a best practice until 31 March 2025</i> 	Evolving  requirement
3.4	3.5.1	Removed pads from the “Index tokens and pads” bullet for rendering PAN unreadable.	Evolving  requirement
	3.5.1.1	New requirement for keyed cryptographic hashes when hashing is used to render PAN unreadable. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
	3.5.1.2	New requirement that disk-level or partition-level encryption is used only to render PAN unreadable on removable electronic media or, if used on non-removable electronic media, the PAN is also rendered unreadable via a mechanism that meets Requirement 3.5.1. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
3.5.1	3.6.1.1	New requirement bullet for service providers only to include in the documented description of the cryptographic architecture that use of the same cryptographic keys in production and test environments is prevented. <i>This bullet is a best practice until 31 March 2025.</i>	Evolving  requirement



Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Requirement 4			
Requirement 4 - General		Updated principal requirement title to reflect the focus on “strong cryptography” to protect transmissions of cardholder data.	Clarification or guidance
	4.1.2	New requirement for roles and responsibilities. <i>This requirement is effective immediately for all v4.0 assessments.</i>	Evolving  requirement
4.1	4.2.1	New requirement bullet to confirm certificates used for PAN transmissions over open, public networks are valid and not expired or revoked. <i>This bullet is a best practice until 31 March 2025.</i>	Evolving  requirement
	4.2.1.1	New requirement to maintain an inventory of trusted keys and certificates. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
Requirement 5			
Requirement 5 - General		Updated principal requirement title to reflect the focus on protecting all systems and networks from malicious software.	Clarification or guidance
		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.	Evolving  requirement
	5.1.2	New requirement for roles and responsibilities. <i>This requirement is effective immediately for all v4.0 assessments.</i>	Evolving  requirement
5.1.2	5.2.3	Clarified requirement by changing focus to “system components that are not at risk for malware.”	Clarification or guidance
	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. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
5.2	5.3.1 5.3.2 5.3.4	Split one requirement into three to focus each requirement on one area: <ul style="list-style-type: none"> • Keeping the malware solution current via automatic updates, • Performing periodic scans and active or real-time scans (with a new option for continuous behavioral analysis), • Generation of audit logs by the malware solution. 	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
	5.3.2.1	New requirement to define the frequency of periodic malware scans in the entity's targeted risk analysis. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
	5.3.3	New requirement for a malware solution for removable electronic media. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
	5.4.1	New requirement to detect and protect personnel against phishing attacks. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
Requirement 6			
Requirement 6 - General		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.	Clarification or guidance
	6.1.2	New requirement for roles and responsibilities. This requirement is effective immediately for all v4.0 assessments.	Evolving  requirement
6.3	6.2.1	Moved requirement for developing software securely to align all software development content under Requirement 6.2.	Structure or format
		Replaced "internal and external" with "bespoke and custom" software. Clarified that this requirement applies to software developed for or by the entity for the entity's own use and does not apply to third-party software.	Clarification or guidance
6.5	6.2.2	Moved the elements of Requirement 6.5 for training of software developers to align all software development content under Requirement 6.2. Clarified training requirements for software development personnel.	Clarification or guidance
6.3.2	6.2.3 6.2.3.1	Moved requirement for reviewing custom software prior to release to align all software development content under Requirement 6.2. Split requirement to separate general code review practices from those needed if manual code reviews are performed.	Clarification or guidance







Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
6.5.1 – 6.5.10	6.2.4	<p>Moved requirements for addressing common coding vulnerabilities to align all software development content under Requirement 6.2.</p> <p>Combined methods to prevent or mitigate common software attacks into a single requirement and generalized the language describing each type of attack.</p>	Clarification or guidance
6.1 6.2	6.3	Moved requirements for identifying security vulnerabilities and protecting system components from vulnerabilities via patching under Requirement 6.3.	Structure or format
6.1	6.3.1	Added a bullet to clarify applicability to vulnerabilities for bespoke and custom and third-party software.	Clarification or guidance
	6.3.2	<p>New requirement to maintain an inventory of bespoke and custom software.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p>	Evolving  requirement
6.6	6.4.1	Moved requirement for addressing new threats and vulnerabilities for public-facing web applications under Requirement 6.4.	Structure or format
	6.4.2	<p>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.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p>	Evolving  requirement
	6.4.3	<p>New requirement for management of all payment page scripts that are loaded and executed in the consumer's browser.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p>	Evolving  requirement
6.3.1 6.4 6.4.1 – 6.4.6	6.5.1 – 6.5.6	Moved and combined requirements for changes to system components under Requirement 6.5.	Structure or format
6.4	6.5.3 6.5.4 6.5.5 6.5.6	Removed requirement for specific documented procedures and added testing procedures to verify policies and procedures to each related requirement.	Clarification or guidance
6.4.1	6.5.3	Changed term from “development/test and production” to “production and pre-production” environments.	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
6.4.2	6.5.4	<p>Changed term from “development/test and production” to “production and pre-production” environments.</p> <p>Changed term “separation of duties” and clarified that separation of roles and functions between production and pre-production is intended to provide accountability so that only approved changes are deployed.</p>	Clarification or guidance
6.4.3	6.5.5	<p>Changed term from “testing or development” to “pre-production” environments.</p> <p>Clarified that live PANs are not used in pre-production environments except where all applicable PCI DSS requirements are in place.</p>	Clarification or guidance
Requirement 7			
Requirement 7 - General		Updated principal requirement title to include system components and cardholder data.	Clarification or guidance
	7.1.2	<p>New requirement for roles and responsibilities.</p> <p><i>This requirement is effective immediately for all v4.0 assessments.</i></p>	Evolving requirement ●
7.1	7.2.1 7.2.2 7.2.3	Removed requirement for specific documented procedures and added testing procedures to verify policies and procedures to each related requirement.	Clarification or guidance
7.1.1	7.2.1	Clarified requirement is about defining an access control model.	Clarification or guidance
7.1.2 7.1.3	7.2.2	Combined requirements for assigning access based on job classification and function, and least privileges.	Structure or format
7.1.4	7.2.3	Clarified requirement is about approval of required privileges by authorized personnel.	Clarification or guidance
	7.2.4	<p>New requirement for review of all user accounts and related access privileges.</p> <p>This requirement is a best practice until 31 March 2025.</p>	Evolving requirement ●
	7.2.5	<p>New requirement for assignment and management of all application and system accounts and related access privileges.</p> <p>This requirement is a best practice until 31 March 2025.</p>	Evolving requirement ●
	7.2.5.1	<p>New requirement for review of all access by application and system accounts and related access privileges.</p> <p>This requirement is a best practice until 31 March 2025.</p>	Evolving requirement ●




Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
8.7	7.2.6	Moved requirement since it aligns better with the content in Requirement 7.	Structure or format
7.2		Removed “null” requirement (all content pointed to other requirements).	Structure or format
Requirement 8			
Requirement 8 - General		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).	Clarification or guidance
		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.	Structure or format
	8.1.2	New requirement for roles and responsibilities. <i>This requirement is effective immediately for all v4.0 assessments.</i>	Evolving requirement 
8.1.1	8.2.1	Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Clarification or guidance
8.5	8.2.2	Changed focus of requirement to allow use of shared authentication credentials, but only on an exception basis.	Evolving requirement 
		Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Clarification or guidance
8.5 8.5.1	8.2.2 8.2.3	Moved requirements for group, shared, or generic accounts and for service providers with remote access to customer premises under Requirement 8.2.	Structure or format
8.1.8	8.2.8	Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Structure or format
8.2	8.3.1	Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Structure or format

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
8.1.6 8.1.7	8.3.4	Merged requirements and moved under Requirement 8.3 Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Structure or format
		Increased the number of invalid authentication attempts before locking out a user ID from six to 10 attempts.	Evolving  requirement
8.2.6	8.3.5	Clarified that this requirement applies only if passwords/passphrases are used as an authentication factor to meet Requirement 8.3.1.	Clarification or guidance
8.2.3	8.3.6	<p>New requirement to increase password length from a minimum length of seven characters to minimum length of 12 characters (or if the system does not support 12 characters, a minimum length of eight characters).</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p> <p>Clarified that, until 31 March 2025, passwords must be a minimum length of at least seven characters in accordance with v3.2.1 Requirement 8.2.3.</p> <p>Clarified that this requirement applies only if passwords/passphrases are used as an authentication factor to meet Requirement 8.3.1.</p> <p>Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.</p>	Evolving  requirement
8.2.5	8.3.7	Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.	Structure or format
8.4	8.3.8	Moved content about communicating user authentication policies and procedures under Requirement 8.3.	Structure or format

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
8.2.4	8.3.9	<p>Clarified that this requirement applies only if passwords/passphrases are used as an authentication factor to meet Requirement 8.3.1.</p> <p>Added a note that this requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.</p> <p>Added a note that requirement does not apply to service providers' customer accounts, but does apply to accounts for service provider personnel.</p>	Clarification or guidance
		<p>Added the option to determine access to resources automatically by dynamically analyzing the security posture of accounts, instead of changing passwords/passphrases at least once every 90 days.</p>	Evolving ● requirement
8.2.4.b	8.3.10	<p>Moved content from a former testing procedure to a requirement for service providers to provide guidance to customers about changing passwords/passphrases.</p> <p>Added a note that this requirement will be superseded by Requirement 8.3.10.1 once Requirement 8.3.10.1 becomes effective.</p>	Structure or format
	8.3.10.1	<p>New requirement for service providers only – if passwords/passphrases are the only authentication factor for customer user access, then passwords/passphrases are either changed at least once every 90 days or access to resources is automatically determined by dynamically analyzing the security posture of the accounts.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p> <p>Added a note that this requirement does not apply to accounts of consumer users accessing their payment card information.</p> <p>Added a note that this requirement will supersede Requirement 8.3.10 once it becomes effective, and until that date, service providers may meet either Requirement 8.3.10 or 8.3.10.1.</p>	Evolving ● requirement
8.6	8.3.11	<p>Moved requirement about authentication factors such as physical or logical security tokens, smart cards, and certificates under Requirement 8.3.</p>	Structure or format
8.3		<p>Removed "null" requirement (all content pointed to other requirements).</p>	Structure or format

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
	8.4.2	<p>New requirement to implement multi-factor authentication (MFA) for all access into the CDE.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p> <p>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.</p>	Evolving  requirement
	8.5.1	<p>New requirement for secure implementation of multi-factor authentication systems.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p>	Evolving  requirement
	8.6.1	<p>New requirement for management of system or application accounts that can be used for interactive login.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p>	Evolving  requirement
	8.6.2	<p>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.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p>	Evolving  requirement
	8.6.3	<p>New requirement for protecting passwords/passphrases for application and system accounts against misuse.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p>	Evolving  requirement
8.7	7.2.6	Moved requirement since it aligns better with the content in Requirement 7.	Structure or format
Requirement 9			
Requirement 9 - General		<p>In the overview, clarified the three different areas covered in Requirement 9 (sensitive areas, CDE, and facilities).</p> <p>Throughout, clarified whether each requirement applies to the CDE, sensitive areas, or facilities.</p>	Clarification or guidance
	9.1.2	<p>New requirement for roles and responsibilities.</p> <p><i>This requirement is effective immediately for all v4.0 assessments.</i></p>	Evolving  requirement
9.1	9.2.4	Added a requirement to address a former testing procedure bullet to restrict access to consoles in sensitive areas via locking when not in use.	Clarification or guidance








Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
9.2	9.3.1 9.3.2	Split requirement for identifying personnel and visitors into separate requirements, Requirements 9.3.1 and 9.3.2 respectively.	Structure or format
9.4 9.4.1 9.4.2	9.3.2	Combined requirements for authorizing and managing visitor access together in Requirement 9.3.2.	Structure or format
9.5 9.5.1	9.4.1 9.4.1.1 9.4.1.2	Removed requirement for procedures to physically secure media (9.5) and merged the procedures into the related requirements. Split requirement for storing media backups in a secure location and reviewing the security of the offline backup location at least every 12 months into 2 requirements.	Clarification or guidance
9.6 9.6.1 9.6.2 9.6.3	9.4.2 9.4.3 9.4.4	Removed requirement for procedures for internal and external distribution of media (9.6) and merged the procedures into the related requirements.	Clarification or guidance
9.7 9.7.1	9.4.5 9.4.5.1	Removed requirement for procedures for strict control over storage and accessibility of media (9.7) and merged the procedures into the related requirements. Split requirement for maintaining media inventory logs and conducting media inventories annually into 2 requirements.	Clarification or guidance
9.8 9.8.1 9.8.2	9.4.6 9.4.7	Removed requirement for procedures for media destruction when media is no longer needed (9.8) and merged the procedures into the related requirements. Clarified options for destroying media when no longer needed includes either destruction of electronic media or rendering cardholder data unrecoverable.	Clarification or guidance
9.9	9.5.1	Clarified the focus of the requirement is on “Point-of-interaction (POI) devices that capture payment card data via direct physical interaction with the payment card form factor.” Clarified that requirement applies to deployed POI devices used in card-present transactions.	Clarification or guidance
	9.5.1.2.1	New requirement to define the frequency of periodic POI device inspections based on the entity’s targeted risk analysis. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving ● requirement





Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Requirement 10			
Requirement 10 - General		Updated principal requirement 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.	Clarification or guidance
	10.1.2	New requirement for roles and responsibilities. <i>This requirement is effective immediately for all v4.0 assessments.</i>	Evolving  requirement
10.2		Removed "null" requirement (all content pointed to other requirements).	Structure or format
10.5		Removed "null" requirement (all content pointed to other requirements).	Structure or format
10.5.1 – 10.5.5	10.3.1 – 10.3.4	Moved audit log protection requirements under Requirement 10.3.	Structure or format
10.5.3 10.5.4	10.3.3	Combined requirements to align similar topics.	Structure or format
10.6		Removed "null" requirement (all content pointed to other requirements).	Structure or format
10.6.1 – 10.6.3	10.4.1 – 10.4.3	Moved requirements for audit log reviews under Requirement 10.4.	Structure or format
	10.4.1.1	New requirement for the use of automated mechanisms to perform audit log reviews. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
	10.4.2.1	New requirement for a targeted risk analysis to define the frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
10.7	10.5.1	Moved requirement for audit log history to 10.5.1.	Structure or format
10.4 10.4.1 – 10.4.3	10.6.1 – 10.6.3	Moved and reorganized requirements for time synchronization under 10.6.	Structure or format
10.8	10.7.1	Moved requirement <i>for service providers</i> to detect, alert, and promptly address failures of critical control systems to Requirement 10.7.1.	Structure or format




Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
	10.7.2	<p>New requirement for all entities to detect, alert, and promptly address failures of critical security control systems.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p> <p>This new requirement applies to all entities - it includes two additional critical security controls not included in Requirement 10.7.1 for service providers.</p>	Evolving ● requirement
10.8.1	10.7.3	<p>New requirement to respond promptly to failures of any critical security controls.</p> <p>For service providers: this is current PCI DSS v3.2.1 requirement.</p> <p>For all other (non-service provider) entities: this is a new requirement.</p> <p><i>This requirement is a best practice (for non-service providers) until 31 March 2025.</i></p>	Evolving ● requirement





Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Requirement 11			
Requirement 11 - General		Minor update to principal requirement title.	Clarification or guidance
	11.1.2	New requirement for roles and responsibilities. <i>This requirement is effective immediately for all v4.0 assessments.</i>	Evolving requirement ●
11.1	11.2.1	Clarified the intent of the requirement is to manage both authorized and unauthorized wireless access points. Clarified that this requirement applies even when a policy exists to prohibit the use of wireless technology.	Clarification or guidance
	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. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving requirement ●
	11.3.1.2	New requirement to perform internal vulnerability scans via authenticated scanning. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving requirement ●
11.2.3	11.3.1.3 11.3.2.1	Separated requirement to perform internal and external vulnerability scans and rescans after any significant changes into a requirement for internal scans (11.3.1.3) and external scans (11.3.2.1).	Structure or format
11.3	11.4.1	Clarified the following: <ul style="list-style-type: none"> 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
11.3.3	11.4.4	Clarified that penetration test findings are corrected in accordance with the entity's assessment of the risk posed by the security issue.	Clarification or guidance
	11.4.7	New requirement for multi-tenant service providers to support their customers for external penetration testing. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving requirement ●



Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
	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. <i>This requirement is a best practice until 31 March 2025.</i>	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. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving ● requirement
11.2		Removed "null" requirement (all content pointed to other requirements).	Structure or format
11.1.2	12.10.5	Moved requirement for incident response procedures if unauthorized wireless access points are detected to align with other incident response items.	Structure or format
11.5.1	12.10.5	Moved requirement to respond to alerts generated by the change-detection solution to align with other the incident response items.	Structure or format
Requirement 12			
Requirement 12 - General		Updated principal requirement title to reflect that the focus is on organizational policies and programs that support information security.	Clarification or guidance
12.2		Removed requirement for a formal organization-wide risk assessment and replaced with specific targeted risk analyses (12.3.1 and 12.3.2).	Evolving ● requirement
12.4	12.1.3	Added formal acknowledgment by personnel of their responsibilities.	Evolving ● requirement
12.5 12.5.1 – 12.5.5	12.1.4	Clarified that responsibilities are formally assigned to a Chief Information Security Officer or other knowledgeable member of executive management. Merged requirements for formally assigning responsibility for information security.	Clarification or guidance
12.3 12.3.1 – 12.3.9	12.2.1	Clarified the intent of the requirement is for acceptable use policies for end-user technologies. Merged and removed requirements to focus on explicit management approval, acceptable uses of technologies, and a list of hardware and software products approved by the company for employee use.	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
12.3.10	3.4.2	Removed requirement and added new Requirement 3.4.2 for technical controls to prevent copy and/or relocation of PAN when using remote-access technologies.	Evolving  requirement
	12.3.1	New requirement to perform a targeted risk analysis for any PCI DSS requirement that provides flexibility for how frequently it is performed. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  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. <i>This requirement is effective immediately for all entities undergoing a v4.0 assessment and using a customized approach.</i>	Evolving  requirement
	12.3.3	New requirement to document and review cryptographic cipher suites and protocols in use at least once every 12 months. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
	12.3.4	New requirement to review hardware and software technologies in use at least once every 12 months. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
12.11 12.11.1	12.4.2 12.4.2.1	Moved requirements for reviews to confirm that personnel are performing PCI DSS tasks in accordance with policies and procedures under Requirement 12.4, to align with other requirements for managing PCI DSS compliance activities.	Structure or format
2.4	12.5.1	Moved under Requirement 12.5 to align with other requirements for documenting and validating PCI DSS scope.	Structure or format
	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. <i>This requirement is effective immediately for all v4.0 assessments.</i>	Evolving  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. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
	12.5.3	New requirement for service providers for a documented review of the impact to PCI DSS scope and applicability of controls upon significant changes to organizational structure. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
12.6	12.6.1	Clarified that the intent is that all personnel are aware of the entity's information security policy and their role in protecting cardholder data.	Clarification or guidance
	12.6.2	New requirement to review and update (as needed) the security awareness program at least once every 12 months. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
12.6.1 12.6.2	12.6.3	Merged requirements for security awareness training.	Structure or format
	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. <i>This requirement is a best practice until 31 March 2025.</i>	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. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
12.8		Removed "null" requirement (all content pointed to other requirements).	Structure or format
12.8.1 – 12.8.5	12.8.1 – 12.8.5	Replaced "Service Provider" with Third-Party Service Provider (TPSP). Clarified that the use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.	Clarification or guidance
12.8.2	12.8.2	Replaced "Service Provider" with Third-Party Service Provider (TPSP).	Clarification or guidance
12.8.3	12.8.3	Replaced "Service Provider" with Third-Party Service Provider (TPSP).	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
12.8.4	12.8.4	Replaced “Service Provider” with Third-Party Service Provider (TPSP). Clarified that where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity, the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also “not in place” for the entity.	Clarification or guidance
12.8.5	12.8.5	Replaced “Service Provider” with Third-Party Service Provider (TPSP). Clarified that the information about PCI DSS requirements managed by the TPSP and the entity should include any that are shared between the TPSP and the entity.	Clarification or guidance
	12.9.2	New requirement for service providers to support their customers’ requests for information to meet Requirements 12.8.4 and 12.8.5. <i>This requirement is effective immediately for all v4.0 assessments.</i>	Evolving  requirement
12.10		Removed “null” requirement (all content pointed to other requirements).	Structure or format
12.10.1	12.10.1	Replaced “system breach” and “compromise” with “suspected or confirmed security incident.”	Clarification or guidance
12.10.3	12.10.3	Replaced “alerts” with “suspected or confirmed security incidents.”	Clarification or guidance
12.10.4	12.10.4	Replaced “system breach” with “suspected or confirmed security incidents.”	Clarification or guidance
	12.10.4.1	New requirement to perform a targeted risk analysis to define the frequency of periodic training for incident response personnel. <i>This requirement is a best practice until 31 March 2025.</i>	Evolving  requirement
12.10.5 11.1.2 11.5.1	12.10.5	Merged requirements and updated the security monitoring systems to be monitored and responded to as part of the incident response plan to include the following: <ul style="list-style-type: none"> • Detection of unauthorized wireless access points (former 11.1.2), • Change-detection mechanism for critical files (former 11.5.1), • New requirement bullet for use of a change- and tamper-detection mechanism for payment pages (relates to new requirement 11.6.1). <i>This bullet is a best practice until 31 March 2025.</i>	Evolving  requirement

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
	12.10.7	<p>New requirement for incident response procedures to be in place and initiated upon detection of stored PAN anywhere it is not expected.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p>	Evolving 
Appendix A1			
Appendix A1 - General		<p>Updated principal requirements title to reflect focus on multi-tenant service providers.</p> <p>Updated requirement overview to describe multi-tenant service providers and their environments, and to clarify responsibilities between multi-tenant service providers and their customers.</p> <p>Updated “shared hosting provider” to “multi-tenant hosting provider” throughout.</p>	Clarification or guidance
A1		Removed “null” requirement (all content pointed to other requirements).	Structure or format
	A1.1.1	<p>New requirement for to implement logical separation between providers’ environments and customers’ environments.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p>	Evolving 
	A1.1.4	<p>New requirement to confirm, via penetration testing, the effectiveness of logical separation controls used to separate customer environments.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p>	Evolving 
	A1.2.3	<p>New requirement for the implementation of processes and mechanisms for reporting and addressing suspected or confirmed security incidents and vulnerabilities.</p> <p><i>This requirement is a best practice until 31 March 2025.</i></p>	Evolving 
A1.4	A1.2.2	Replaced “compromise” with “suspected or confirmed security incident”	Clarification or guidance
Appendix A2			
The only changes made to Appendix A2 were to add the requirement description heading at A2.1 and to renumber the three requirements as A2.1.1, A2.1.2, and A2.1.3.			Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
Appendix A3			
Appendix A3 - General		<p>Clarified that other PCI standards may reference completion of this Appendix.</p> <p>Clarified that not all PCI DSS requirements apply to all entities that undergo a PCI DSS assessment, which is why some PCI DSS requirements are duplicated in this Appendix. Any questions about this Appendix should be addressed to acquirers or payment brands.</p>	Clarification or guidance
A3.2.1	A3.2.1	Updated the elements included for PCI DSS scope documentation and confirmation to align with new PCI DSS Requirement 12.5.2.	Evolving  requirement
	A3.3.1	<p>New requirement bullet to detect, alert, and report failures of automated log review mechanisms.</p> <p>New requirement bullet to detect, alert, and report failures of automated code review tools.</p> <p><i>These bullets are best practices until 31 March 2025.</i></p>	Evolving  requirement
Appendix B: Compensating Controls	Appendix B: Compensating Controls	<p>Clarified that compensating controls may be considered when an entity cannot meet a PCI DSS requirement explicitly as written, due to “legitimate and documented technical or business constraints.”</p> <p>Updated item 2 to mention the Customized Approach Objective and its use to understand the intent of most PCI DSS requirements.</p> <p>Clarified the intent of item 4 is to address the risk imposed by not adhering to the PCI DSS requirement.</p> <p>Added item 6 to clarify that compensating controls are used to address requirements currently and in the future, and they cannot be used to address a requirement missed in the past.</p>	Clarification or guidance
Appendix C: Compensating Controls Worksheet	Appendix C: Compensating Controls Worksheet	<p>Clarified that the intent is for the entity to use the worksheet to define its compensating controls.</p> <p>Updated item 1 to “Document the legitimate technical or business constraints precluding compliance with the original requirement.”</p> <p>Reordered the worksheet items to move item 4 to item 2.</p> <p>Updated item 3 to mention the Customized Approach Objective, and split item into two parts to “Define the objective of the original control” and to “Identify the objective met by the compensating control.”</p> <p>Removed the Compensating Control Worksheet - Completed Example. An updated completed example will be included in a separate guidance document.</p>	Clarification or guidance
	Appendix D: Customized Approach	New Appendix to explain and provide instructions for the Customized Approach.	Clarification or guidance

Section		Description of Change	Change Type
PCI DSS v3.2.1	PCI DSS v4.0		
	Appendix E: Sample Templates to Support Customized Approach	<p>New Appendix for example templates for the controls matrix and targeted risk analysis, to be documented by the entity as part of the customized approach.</p> <p>Clarified that entities are not required to follow the specific template formats, but must provide all information as defined in each template.</p> <p>Includes two templates:</p> <ul style="list-style-type: none"> • E1 Sample Controls Matrix Template • E2 Sample Targeted Risk Analysis Template. 	Clarification or guidance
	Appendix F: Leveraging the PCI Software Security Framework to Support Requirement 6	<p>New Appendix to describe how an entity can meet several requirements in Requirement 6 by use of bespoke or custom software that is developed and maintained in accordance with one of PCI SSC's Secure Software Standards.</p>	Clarification or guidance
	Appendix G: PCI DSS Glossary of Terms, Abbreviations, and Acronyms	<p>New Appendix for the PCI DSS v4.0 Glossary.</p> <p>General updates to the Glossary include:</p> <ul style="list-style-type: none"> • Added new terms based on updated requirements or based on feedback, • Removed common terms that can be readily found with other sources, • Removed terms not used in PCI DSS v4.0, • Shortened acronym definitions. 	Clarification or guidance
Appendix D: Segmentation and Sampling of Business Facilities/ System Components		Removed Appendix and moved former content to sections titled "Segmentation" and "For Assessors: Sampling for PCI DSS Assessments."	Clarification or guidance

6 ● Summary of New Requirements

As noted in the table below, the new requirements included in PCI DSS v4.0 are either:

- Effective immediately for all PCI DSS v4.0 assessments.
- OR
- Best practices until 31 March 2025, after which they become effective.

● New Requirement		Applicable to		Effective Date ●	
		All ● Entities	Service ● Providers Only	Immediately for all v4.0 Assessments ●	31 March 2025
2.1.2	Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	✓			
3.1.2	Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	✓		✓ ●	
3.2.1	Any SAD stored prior to completion of authorization is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes.	✓			✓ ●
3.3.2	SAD stored electronically prior to completion of authorization is encrypted using strong cryptography.	✓			✓
3.3.3	SAD stored by issuers is encrypted using strong cryptography.		✓ ¹ ●		✓
3.4.2	Technical controls to prevent copy and/or relocation of PAN when using remote-access technologies except with explicit authorization.	✓			✓
3.5.1.1	Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN with associated key-management processes and procedures.	✓			✓
3.5.1.2	Implementation of disk-level or partition-level encryption when used to render PAN unreadable.	✓			✓
3.6.1.1	A documented description of the cryptographic architecture includes prevention of the use of cryptographic keys in production and test environments.		✓		✓

¹ Applicable only to issuers and companies that support issuing services and store sensitive authentication data.

New Requirement	Applicable to		Effective Date	
	All Entities	Service Providers Only	Immediately for all v4.0 Assessments	31 March 2025
4.1.2	Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	✓		✓
4.2.1	Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked.	✓		✓
4.2.1.1	An inventory of the entity's trusted keys and certificates is maintained.	✓		✓
5.1.2	Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	✓		✓
5.2.3.1	A targeted risk analysis is performed to determine frequency of periodic evaluations of system components identified as not at risk for malware.	✓		✓
5.3.2.1	A targeted risk analysis is performed to determine frequency of periodic malware scans.	✓		✓
5.3.3	Anti-malware scans are performed when removable electronic media is in use.	✓		✓
5.4.1	Mechanisms are in place to detect and protect personnel against phishing attacks.	✓		✓
6.1.2	Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	✓		✓
6.3.2	Maintain an inventory of bespoke and custom software to facilitate vulnerability and patch management.	✓		✓
6.4.2	Deploy an automated technical solution for public-facing web applications that continually detects and prevents web-based attacks.	✓		✓
6.4.3	Manage all payment page scripts that are loaded and executed in the consumer's browser.	✓		✓
7.1.2	Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	✓		✓
7.2.4	Review all user accounts and related access privileges appropriately.	✓		✓

New Requirement		Applicable to		Effective Date	
		All Entities	Service Providers Only	Immediately for all v4.0 Assessments	31 March 2025
7.2.5	Assign and manage all application and system accounts and related access privileges appropriately.	✓			✓
7.2.5.1	Review all access by application and system accounts and related access privileges.	✓			✓
8.1.2	Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	✓		✓	
8.3.6	Minimum level of complexity for passwords when used as an authentication factor.	✓			✓
8.3.10.1	If passwords/passphrases are the only authentication factor for customer user access, passwords/passphrases are changed at least every 90 days or the security posture of accounts is dynamically analyzed to determine real-time access to resources.		✓		✓
8.4.2	Multi-factor authentication for all access into the CDE.	✓			✓
8.5.1	Multi-factor authentication systems are implemented appropriately.	✓			✓
8.6.1	Manage interactive login for accounts used by systems or applications.	✓			✓
8.6.2	Passwords/passphrases used for interactive login for application and system accounts are protected against misuse.	✓			✓
8.6.3	Passwords/passphrases for any application and system accounts are protected against misuse.	✓			✓
9.1.2	Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	✓		✓	
9.5.1.2.1	A targeted risk analysis is performed to determine frequency of periodic POI device inspections.	✓			✓
10.1.2	Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	✓		✓	
10.4.1.1	Audit log reviews are automated.	✓			✓

New Requirement		Applicable to		Effective Date	
		All Entities	Service Providers Only	Immediately for all v4.0 Assessments	31 March 2025
10.4.2.1	A targeted risk analysis is performed to determine frequency of log reviews for all other system components.	✓			✓
10.7.2	Failures of critical security control systems are detected, alerted, and addressed promptly.	✓			✓
10.7.3	Failures of critical security control systems are responded to promptly.	✓			✓
11.1.2	Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	✓		✓	
11.3.1.1	Manage all other applicable vulnerabilities (those not ranked as high-risk or critical).	✓			✓
11.3.1.2	Internal vulnerability scans are performed via authenticated scanning.	✓			✓
11.4.7	Multi-tenant service providers support their customers for external penetration testing.		✓		✓
11.5.1.1	Covert malware communication channels detect, alert and/or prevent, and address via intrusion-detection and/or intrusion-prevention techniques.		✓		✓
11.6.1	A change-and-tamper-detection mechanism is deployed for payment pages.	✓			✓
12.3.1	A targeted risk analysis is documented to support each PCI DSS requirement that provides flexibility for how frequently it is performed.	✓			✓
12.3.2	A targeted risk analysis is performed for each PCI DSS requirement that is met with the customized approach.	✓		✓	
12.3.3	Cryptographic cipher suites and protocols in use are documented and reviewed.	✓			✓
12.3.4	Hardware and software technologies are reviewed.	✓			✓
12.5.2	PCI DSS scope is documented and confirmed at least once every 12 months.	✓		✓	

New Requirement		Applicable to		Effective Date	
		All Entities	Service Providers Only	Immediately for all v4.0 Assessments	31 March 2025
12.5.2.1	PCI DSS scope is documented and confirmed at least once every six months and upon significant changes.		✓		✓
12.5.3	The impact of significant organizational changes on PCI DSS scope is documented and reviewed and results are communicated to executive management.		✓		✓
12.6.2	The security awareness program is reviewed at least once every 12 months and updated as needed.	✓			✓
12.6.3.1	Security awareness training includes awareness of threats that could impact the security of the CDE, to include phishing and related attacks and social engineering.	✓			✓
12.6.3.2	Security awareness training includes awareness about acceptable use of end-user technologies.	✓			✓
12.9.2	TPSPs support customers' requests to provide PCI DSS compliance status and information about PCI DSS requirements that are the responsibility of the TPSP.		✓	✓	
12.10.4.1	A targeted risk analysis is performed to determine frequency of periodic training for incident response personnel.	✓			✓
12.10.5	The security incident response plan includes alerts from the change- and tamper-detection mechanism for payment pages.	✓			✓
12.10.7	Incident response procedures are in place and initiated upon detection of PAN.	✓			✓
A1.1.1	The multi-tenant service provider confirms access to and from customer environment is logically separated to prevent unauthorized access.		✓		✓
A1.1.4	The multi-tenant service provider confirms effectiveness of logical separation controls used to separate customer environments at least once every six months via penetration testing.		✓		✓

New Requirement		Applicable to		Effective Date	
		All Entities	Service Providers Only	Immediately for all v4.0 Assessments	31 March 2025
A1.2.3	The multi-tenant service provider implements processes or mechanisms for reporting and addressing suspected or confirmed security incidents and vulnerabilities.		✓		✓
A3.3.1	Failures of the following are detected, alerted, and reported in a timely manner: Automated log review mechanisms Automated code review tools.	✓			✓
Totals:		53	11	13	51
Grand Total: 64					