Payment Card Industry

Data Security Standard

Summary of Changes from PCI DSS Version 4.0 to 4.0.1

August 2024

Document Changes

Date	Revision	Description
June 2024		Initial release of the PCI DSS v4.0 to v4.0.1 Summary of Changes.
August 2024	1	Errata update to add “Clarification or Guidance” Change Type for Requirement 6.5.5.

Table of Contents

1 Introduction

This document provides a summary and description of the changes from PCI DSS v4.0 to PCI DSS v4.0.1 and does not detail all document revisions.

The tables included herein summarize the changes for PCI DSS v4.0.1 from PCI DSS v4.0. The summary is organized as follows:

- Change Types- provides an overview of the types of changes.
- *Summary of General Changes* - includes descriptions of general changes made throughout.
- *Summary of General Changes to PCI DSS Introductory Sections* - includes descriptions of changes made for each affected section.
- *Summary of Changes to PCI DSS Requirements* - includes descriptions of changes made throughout the requirements, testing procedures, and guidance.

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. *Note that there were no changes categorized as "Evolving Requirement" in this version of PCI DSS.*
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 General Changes

Description of Changes from PCI DSS v4.0 to v4.0.1
Correct typographical and other minor errors (including formatting errors, missing headers, etc.).
Update and clarify guidance, including changes to align with subsequent publications (e.g., the v4.0 Quick Reference Guide and recently published FAQs).
Remove *Definitions* in Guidance if also included in the Glossary and refer to Glossary (Appendix G) instead.
Add references to the Glossary for newly defined glossary terms and for existing glossary terms that did not previously have references.
Change "impact the security of the CDE" to "impact the security of cardholder data and/or sensitive authentication data", throughout the standard where appropriate.
Update Testing Procedures to align with updated Requirement wording, as needed.

4 Summary of General Changes to PCI DSS Introductory Sections

PCI DSS Section	Change from PCI DSS v4.0 to PCI DSS v4.0.1
Section 3, *Relationship between PCI DSS and PCI SSC Software Standards*	Reword note to reflect the retirement of PA-DSS. Update "Validated Software Vendors" to "Qualified Software Vendors."
Section 4, *Scope of PCI DSS Requirements*	Add sub-section, *When Cardholder Data and/or Sensitive Authentication Data is Accidentally Received via an Unintended Channel*, to incorporate content previously included in Requirement 4.2.1 Applicability Note.
Section 4, *Scope of PCI DSS Requirements* Sub-section, *Importance of Understanding Responsibilities Between TPSP Customers and TPSPs*	Clarify this sub-section applies if a TPSP provides a service that meets customers' PCI DSS requirements or if that service may impact the security of customers' cardholder data and/or sensitive authentication data.

PCI DSS Section	Change from PCI DSS v4.0 to PCI DSS v4.0.1
	Update reference from *Tips and Tools for Understanding PCI DSS v4.0* to the *Information Supplement: Third-Party Security Assurance*. Clarify that TPSPs must provide customers with documentation about responsibilities only if the TPSP provides a service that meets customers' PCI DSS requirements or if that service may impact the security of customers' cardholder data and/or sensitive authentication data.
Section 7, *Description of Timeframes Used in PCI DSS Requirements*	Clarify the Significant Change description. Clarify that it is considered an initial PCI DSS assessment only when an entity is being assessed for the first time against a PCI DSS requirement with a defined timeframe.
Section 8, *Approaches for Implementing and Validating PCI DSS*	Update Customized Approach references to include the *Sample Templates to Support the Customized Approach* on the PCI SSC website. Update the colors and font in Figure 4 and update from "ROC Reporting Template" to "ROC Template."
Section 13, *Additional References*	Remove URL links.
Section 14, *PCI DSS Versions*	Remove reference to PCI DSS v3.2.1 since it is now retired and clarify that PCI DSS v4.0.1 is the current version. Clarify that questions about the use of previous PCI DSS versions should be directed to organizations that manage compliance programs. Update Table 6 to include v4.0.1 publication date, v4.0 retirement date, and v3.2 information.

5 Summary of Changes to PCI DSS Requirements

PCI DSS Requirement	Description of change	Change Type
Requirement 1		
1.2.2	Add *Purpose* that was erroneously missing.	Clarification or Guidance
Requirement 3		
3.3.1	Update Applicability Note for issuers and companies that support issuing services that any SAD storage is based on "a legitimate and documented business need." Add description of legitimate business need. Add *Good Practice* to address when it may be acceptable to store SAD in non-persistent memory.	Clarification or Guidance
3.3.1, 3.3.1.1, 3.3.1.2, 3.3.1.3	Update requirement from "SAD is not retained after authorization" to "SAD is not stored after authorization" to align with use of "stored" elsewhere in requirement section 3.3.	Clarification or Guidance

PCI DSS Requirement	Description of change	Change Type
3.3.2	Clarify Applicability Note for issuers and companies that support issuing services that any SAD storage is based on "a legitimate and documented business need." Add description of legitimate business need. Update *Definitions* to align the description of "authorization process" with "authorization" definition in the Glossary.	Clarification or Guidance
3.3.3	Add Applicability Note to describe a "legitimate issuing business need" which is aligned with description used in Applicability Notes for Requirements 3.3.1 and 3.3.2. Remove definition previously in Guidance. Remove paragraph that describes the entities for which PCI DSS requirements are intended. Remove *Further Information* since it referred to an outdated ISO standard.	Clarification or Guidance
3.4.2	Clarify *Definitions* that remote access technologies often include tools to disable copy and/or relocation functionality.	Clarification or Guidance
3.5.1	Move Applicability Note that it is relatively trivial to reconstruct PAN data with access to both truncated and hashed versions to *Good Practice*. Update *Purpose* from "The removal of cleartext PAN" to "Rendering PAN unreadable" and remove second, confusingly worded, paragraph. Add to *Good Practice* that implementing keyed cryptographic hashes with associated key management processes and procedures is a valid additional control to prevent correlation.	Clarification or Guidance
3.5.1.1	Add Customized Approach Objective to provide flexibility for meeting this requirement. Remove Applicability Notes duplicated from Requirement 3.5.1 and add that "All Applicability Notes for Requirement 3.5.1 also apply to this requirement." Add an Applicability Note that the requirement will replace the bullet in Requirement 3.5.1 for one-way hashes once its effective date is reached. Add an Applicability Note for system components that generate individual keyed hashes of a PAN for comparison by another system. Update *Purpose* from "The removal of cleartext PAN" to "Rendering PAN unreadable." Remove *Good Practice* and move information to *Purpose*. Add *Examples* related to new Applicability Note for system components that generate individual keyed hashes of a PAN for comparison by another system.	Clarification or Guidance
3.5.1.2	Add a Customized Approach Objective to provide flexibility for meeting this requirement. Add an Applicability Note about the types of encryption methods to which this requirement applies. Add an Applicability Note about how this requirement applies to issuers and those that provide issuing services.	Clarification or Guidance
Requirement 4		
4.2.1	Move the Applicability Note about receiving cardholder data via an unsolicited channel to a new sub-section in Section 4, *Scope of PCI DSS Requirements.* Remove Applicability Note sentence that covered self-signed certificates.	Clarification or Guidance
4.2.2	Add to *Good Practice* about the use of Acceptable Use Policies to manage end-user technologies.	Clarification or Guidance
Requirement 5		
5.4.1	Remove Applicability Note about the automated mechanism to clarify that the requirement does apply to systems providing the mechanism (PCI DSS in general applies to systems that provide security services).	Clarification or Guidance

PCI DSS Requirement	Description of change	Change Type
Requirement 6		
6.3.1	Clarify Applicability Note that this requirement is in addition to performing vulnerability scans according to Requirements 11.3.1 and 11.3.2. Add text from PCI DSS v3.2.1 to *Good Practice* that risk rankings should identify vulnerabilities considered to "high risk" or "critical" to the environment. Update *Good Practice* about including multiple sources of vulnerability information in the entity's process for managing vulnerabilities.	Clarification or Guidance
6.3.3	Update requirement to revert to v3.2.1 language that requirement applies to patches/updates for critical vulnerabilities. Remove language added for v4.0 that the requirement applies to "high-security patches/updates." Remove example of "within three months of release" from the requirement and add it under *Examples*. Clarify that all other applicable security patches/updates are installed as determined by the entity's "assessment of the criticality of the risk to the environment" that the patch addresses. Add to *Good Practice* to recommend entities complete a targeted risk analysis to determine the frequency of installing all other applicable security patches/updates.	Clarification or Guidance
6.4.3	Clarify the requirement bullet that "An inventory of scripts is maintained with written *business or technica*l justification as to why each is necessary." Add three Applicability Notes to clarify how the requirement applies to an entity's webpage(s) and a TPSP's/payment processor's embedded payment page(s)/form(s). Under *Purpose,* add guidance to address situations where it is impractical for scripts to be authorized before a script is changed or added to the page. Under *Good Practice,* add guidance that the entity should expect the TPSP/payment processor to provide evidence that it meets this requirement, where the entity includes a TPSP's/payment processor's embedded payment page/form on its webpage. Remove *Definitions* that explain what "necessary" means for this requirement ("needed for the functionality of the payment page to accept a payment transaction").	Clarification or Guidance
6.5.5	Remove *Good Practice* that explains how entities can minimize storage of live PANs in pre-production. Clarify, under *Definitions*, that live PANs are those issued by, or on behalf of, a payment brand. Remove wording that live PANs have the potential to be used for payment transactions.	Clarification or Guidance
Requirement 8		
Requirement 8 – General	Update the following statement in the Overview and in Applicability Notes for several requirements: "Certain requirements are not intended to apply to user accounts *on point-of-sale terminals* that have access to only once card number at a time to facilitate a single transaction" to add italicized wording and to remove the example included in parentheses.	Clarification or Guidance
8.2.2	Update "account" to "ID" in requirement and guidance to align with the Customized Approach Objective. Update Customized Approach Objective to "group, shared, or generic IDs" to align with requirement.	Clarification or Guidance
8.3.9	Clarify Applicability Note that the requirement does not apply to in-scope system components where MFA is used.	Clarification or Guidance
8.4.1	Move from Applicability Note to *Good Practice* that MFA is a best practice for non-console administrative access to in-scope system components that are not part of the CDE.	Clarification or Guidance

PCI DSS Requirement	Description of change	Change Type
8.4.2	Clarify that the requirement is for all “non-console” access into the CDE. Add Applicability Note that this requirement does not apply to user accounts that are only authenticated with phishing-resistant authentication factors.	Clarification or Guidance
8.4.3	Clarify that this requirement applies to “remote access” rather than the confusing term “remote network access” and move bullets about which types of remote access are included to an Applicability Note. Add “third parties” to testing procedure.	Clarification or Guidance
8.5.1	Add a definition for a replay attack under *Definitions*. Add examples of methods to help protect against replay attacks under *Examples*.	Clarification or Guidance
Requirement 9		
Requirement 9 – General	Add a statement to the Overview that each entity should identify sensitive areas for their environment to ensure appropriate physical security controls are implemented.	Clarification or Guidance
9.2.1	Add Applicability Note that this requirement does not apply to locations that are publicly accessible by consumers (cardholders).	Clarification or Guidance
9.3.4	Clarify requirement is for “visitor logs” rather than “a visitor log” and to “visitor activity *both* with the facility and within sensitive areas.”	Clarification or Guidance
9.5.1	Consolidate Applicability Notes into two bullets to clarify the types of devices to which the requirements at 9.5 do not apply. Move the recommendation from the Applicability Note to *Good Practice*.	Clarification or Guidance
Requirement 10		
10.4.1.1	Add information about establishing a baseline of normal audit activity under *Good Practice*. Add reference to the *Information Supplement: Effective Daily Log Monitoring* under *Further Information*.	Clarification or Guidance
10.5.1	Update *Good Practice* heading to *Purpose* heading to accurately reflect the content in that section.	Structure or format
Requirement 11		
11.2.1	Remove Applicability Note and move under *Purpose* that unauthorized use of wireless technologies is still possible even if the company has a policy to prohibit it.	Clarification or Guidance
11.3.1	Clarify that the requirement applies to vulnerabilities that are “either critical or high-risk.” Add under *Good Practice* that vulnerabilities identified during internal vulnerability scans should be part of the entity's vulnerability management process and include multiple vulnerability sources.	Clarification or Guidance
11.3.1.1	Clarify that the requirement applies to all other vulnerabilities not ranked as "high-risk vulnerabilities or critical vulnerabilities."	Clarification or Guidance
11.3.1.3	Clarify that the requirement applies to vulnerabilities that are “either critical or high-risk.”	Clarification or Guidance
11.3.2	Add to *Good Practice* that vulnerabilities identified during external vulnerability scans should be part of the entity's vulnerability management process and include multiple vulnerability sources. Add reference to the *PCI SSC ASV Program Guide* under *Further Information*.	Clarification or Guidance
11.6.1	Clarify that requirement applies to “*security-impacting* HTTP headers and the *script* contents of payment pages…” Update requirement from “once every seven days” to “weekly” to align with Table 4.	Clarification or Guidance

PCI DSS Requirement	Description of change	Change Type
	Add three Applicability Notes to clarify how the requirement applies to an entity's webpage(s) and a TPSP's/payment processor's embedded payment page(s)/form(s). Expand *Purpose* to include more details about what can be detected when comparing HTTP headers and content of payment pages received by the consumer browser. Under *Good Practice,* add guidance that the entity should expect the TPSP/payment processor to provide evidence that it meets this requirement, where the entity includes a TPSP's/payment processor's embedded payment page/form on its webpage. Clarify *Examples* that mechanisms that detect and report on changes to headers and content of payment pages "*could* include, but are not limited to, *a combination of the following techniques".* Add that the list of mechanisms provided in *Examples* is not exhaustive.	
Requirement 12		
12.1.4	Remove examples of common executive management titles for this role from *Purpose*. Move description that these positions are often at the most senior level of management to *Good Practice.* Add guidance about how information security knowledge for this executive management role can be indicated under *Good Practice*.	Clarification or Guidance
12.3.1	Clarify that the requirement applies only to those PCI DSS requirements that specify completion of a targeted risk analysis. Clarify that the resulting analysis determines and justifies how the entity's defined frequency or processes minimizes the likelihood and/or impact of the threat. Add *Further Information* section to refer to PCI SSC's Targeted Risk Analysis guidance document and sample templates.	Clarification or Guidance
12.3.3	Update third bullet of requirement to "Documentation of a plan" (rather than a "A documented strategy") to align with wording in Requirement 12.3.4. Add to Applicability Note to provide examples of PCI DSS requirements that require use of cryptography.	Clarification or Guidance
12.8.2	Clarify second bullet of requirement that acknowledgements from TPSPs address the TPSPs' responsibility by changing "they" to "TPSPs." Update Applicability Notes as follows: • Clarify the difference between "agreement" and "acknowledgement." • Add that the TPSP's written acknowledgment is confirmation that the TPSP is responsible. • Move examples of evidence that shows a TPSP meets PCI DSS requirements to a separate sentence and add more examples.	Clarification or Guidance
12.9.1	Update second bullet of requirement to reflect same language included at Requirement 12.8.2 about what customers obtain from their TPSPs, to clarify what TPSPs must provide to customers regarding written agreements and acknowledgments. Clarify that acknowledgements from TPSPs address the TPSPs' responsibility by changing "they" to "TPSPs." Update Applicability Notes as follows: • Clarify the difference between "agreement" and "acknowledgement." • Add that the TPSP's written acknowledgment is confirmation that the TPSP is responsible. • Add same Applicability Note included in Requirement 12.8.2 that evidence a TPSP is meeting a PCI DSS requirement is not the same as a written agreement.	Clarification or Guidance

PCI DSS Requirement	Description of change	Change Type
	Update *Purpose* to include wording from PCI DSS v3.2.1 about TPSPs' templates including provision for appropriate acknowledgments.	
12.9.2	Clarify that the first bullet of requirement applies to all TPSPs by removing "for any service the TPSP performs on behalf of customers." Clarify that the second bullet of requirement applies to TPSPs that provide services that meet customer PCI DSS requirements or can impact security of customer account data.	Clarification or Guidance
Appendices		
Appendix A1	Update clause in Overview from "connections to payment gateways and processors" to "payment gateway and processor services offered in a shared environment."	Clarification or Guidance
Appendix A3	Update section in Overview that covers defined timeframes to reflect wording in Section 7 and refers to Section 7 for guidance about initial assessments.	Clarification or Guidance
Appendix D	Update to refer to *PCI DSS v4.x: Sample Templates to Support Customized Approach* on the PCI SSC website rather than Appendix E. Update from "Use of the customized approach must be completed by a QSA or ISA and documented in accordance…" to "Use of the customized approach must be documented by a QSA or ISA in accordance…"	Clarification or Guidance
Appendix E	Remove Customized Approach sample templates and use Appendix E to note the templates are available on the PCI SSC website.	Structure or format
Appendix G	Add definitions for "Legal Exception," "Phishing Resistant Authentication," and "Visitor." Clarify definitions for "Entity," "Interactive Login," and "Payment Page," and "QSA."	Clarification or Guidance