Payment Card Industry
Data Security Standard

PCI DSS ROC Template Summary of Changes from ROC Template v4.0 to v4.0.1

August 2024

Document Changes

Date	Revision	Description
August 2024		Initial release of the PCI DSS ROC Template - Summary of Changes from ROC Template v4.0 to v4.0.1

Table of Contents

1 Introduction

This document provides a summary and description of the Report on Compliance (ROC) Template changes from PCI DSS v4.0 to PCI DSS v4.0.1 and does not detail all document revisions.

This summary is organized as follows:

- *Summary of General Changes to ROC Template* - includes descriptions of general changes made throughout.
- *Summary of Specific Changes to ROC Template* - includes descriptions of changes made for ROC Template Instructions, Part 1 Assessment Overview, and Part II Findings and Observations.

2 Summary of General Changes to ROC Template

Description of PCI DSS v4.0 to v4.0.1 ROC Template Changes
Correct typographical and other minor errors (including formatting errors, missing headers, etc.).
Update language throughout to align with PCI DSS v4.0.1
Remove all pre-formatted text input fields.

3 Summary of Specific Changes to ROC Template

ROC Template Section		Description of Change
v4.0	v4.0.1	
Instructions		
ROC Template Instructions		Clarify that use of the ROC Template is mandatory for all PCI DSS v4.0.1 submissions "when documenting the results of a detailed PCI DSS assessment…"
ROC Sections		Retitle Part II to "Sampling and Evidence, Findings and Observations." Move section 6 to Part II and retitle to "Sampling and Evidence." Add title for section 7 "Findings and Observations." Update last paragraph to reference updated titles for the parts and sections noted above.
-	Method(s) Used	Add section to describe how to report the use of a compensating control or the customized approach.
Figure 1		Replace figure to reflect new requirement layout.
What is the Difference between Not Applicable and Not Tested?		Clarify that both the ROC and AOC(s) must indicate which if any requirements were Not Applicable or Not Tested (formerly only the AOC(s) were cited).

ROC Template Section		Description of Change
v4.0	**v4.0.1**	
Assessment Approach Reporting Options and Figure 2	-	Remove section and figure to reflect new reporting approach for compensating controls and customized approach.
Do's and Don'ts: Reporting Expectations		Add "Do" section bullets to: • Provide a completed Appendix C for any requirements met with a compensating control. • Provide a completed Appendix E for any requirements met with a customized approach. • Read the PCI DSS Applicability Notes and Guidance for each requirement. Update a "Don't" section bullet to clarify that, before copying responses from one requirement to another, the assessor confirms the response is fully applicable to each requirement.
PCI DSS v4.0 Report on Compliance Template	PCI DSS v4.0.1 Report on Compliance Template	Clarify that all instructional content from "this page and all preceding pages" may be deleted prior to finalizing the report.
PCI DSS Customizable cover page		Update "Assessment End Date" to "Date Assessment Ended" to align with Section 1.2 *Date and Timeframe of Assessment*.
Part 1 Assessment Overview		
1.1 Contact Information		Under "Lead Qualified Security Assessor," update "Assessor PCI credentials and certificate number (QSA, Secure Software Assessor, etc." to "Assessor certificate number." Under "Additional Assessors," update "Assessor PCI credentials" to "Assessor certificate number." Under "Assessor Quality Assurance Primary Reviewer," update "QA Reviewer's PCI Credentials" to "QA Reviewer's PCI credentials or certificate number."
1.3 Remote Assessment Activities		Add a reference to *PCI SSC Remote Assessment Guidelines and Procedures*. Remove *Remote Assessment Activities* subsections 1.3.2-1.3.4.
1.8.2 Optional: Additional Assessor comments	-	Remove section *Optional: Additional Assessor comments.*
1.9 Attestation Signatures	-	Remove section *Attestation Signatures*.

ROC Template Section		Description of Change
v4.0	v4.0.1	
2.1 Description of the Entity’s Payment Card Business		Consolidate redundant information about the entity’s payment card business and payment channels. Add a section to separate the description of businesses, services, or functions that store process, or transmit account data from those that could impact the security of account data. Consolidate information about excluded business functions and services into section 3.1.
3.1 Assessor’s Validation of Defined Scope Accuracy		Add “business functions, locations, payment channels, or other” areas to description of areas excluded from the assessment to consolidate information formerly in section 2.1. Update “entity” to “merchant” to clarify that using SAQ eligibility criteria to determine applicability of PCI DSS requirements reported in a ROC is only applicable to merchants.
3.4 Sampling	6.2 Sampling	Move to section 6.2 to clarify its relation to, and align with, the Sample Sets for Reporting table and the section 6 evidence tables.
4.3.1 Storage of SAD		Consolidate table to remove redundancy with section 4.3 Storage of Account Data.
4.4 In-Scope Third-Party Service Providers (TPSPs)s		Remove examples of third-party service providers and add a reference to PCI DSS v4.x Section 4 *Scope of PCI DSS Requirements*
4.7 In-scope Business Functions	-	Remove section *In Scope Business Functions.*
4.8 In-Scope System Component Types	4.7 In-Scope System Component Types	Remove examples of system component types and add a reference to PCI DSS v4.x Section 4 *Scope of PCI DSS Requirements.*
4.9 Sample Sets for Reporting	6.3 Sample Sets for Reporting	Move to section 6.3 to clarify its relation to, and align with, the Sampling Table and the section 6 evidence tables.
5.1 Quarterly External Scan Results		Remove language about ASV scans and “initial PCI DSS compliance” and add a reference to PCI DSS Requirement 11.3.2 for more information about an “initial PCI DSS assessment against this requirement.” Update “quarterly” throughout section.
6 Sampling (Assessment Workpapers)	-	Move section 6 Sampling (Assessment Workpapers) to Part II (see Part II below for details)

ROC Template Section		Description of Change
v4.0	**v4.0.1**	
Part II Sampling and Evidence, Findings and Observations		
Part II Findings and Observations	Part II Sampling and Evidence, Findings and Observations	Retitle Part II to “Sampling and Evidence, Findings and Observations” to account for move of section 6 into Part II.
6 Evidence (Assessment Workpapers)	6 Sampling and Evidence	Retitle to “Sampling and Evidence” to account for move of sampling information into section 6 and to clarify that the ROC is not “workpapers.”
6.1 Evidence Retention		Add a row to identify the assessor who attests that all evidence is stored per the QSA Company’s evidence retention policy.
3.4 Sampling	6.2 Sampling	Move from section 3.4 to clarify its relation to, and align with, the Sample Sets for Reporting table and the section 6 evidence tables.
4.9 Sample Sets for Reporting	6.3 Sample Sets for Reporting	Move from section 4.9 to clarify its relation to, and align with, the Sampling Table and the section 6 evidence tables. Remove column to identify all sub-requirements where the sample set was used.
6.2 Documentation Evidence	6.4 Documentation Evidence	Reorganize sections and retitle column headings to clarify and simplify reporting content.
6.3 Interview Evidence	6.5 Interview Evidence	Reorganize sections, add column for “Title of Workpaper with Interview Notes,” and retitle column heading to clarify and simplify reporting content.
6.4 Observation Evidence	6.6 Other Assessment Evidence	Reorganize sections, combine two evidence tables, retitle column headings to clarify and simplify reporting content.
6.5 System Evidence		
-	7 Findings and Observations	Add header for section 7 Findings and Observations to account for move of section 6 into Part II.
Requirement Layout		Remove Validation Method- Customized Approach reporting rows and add checkbox to note the use of the customized approach.
		Remove Validation Method – Defined Approach reporting rows and add checkbox to note the use of a compensating control.
		Add an instruction that any use of a compensating control or the customized approach must include the corresponding documentation to support the method(s) used.