Payment Card Industry

Data Security Standard

PCI DSS v4.x Report on Compliance Template - Frequently Asked Questions

Revision 2

August 2024

Purpose of document

This document addresses questions about the use of the *Report on Compliance (ROC) Template* for PCI DSS v4.x.

1. Overview of PCI DSS v4.x Reporting

1.1 What has changed in the PCI DSS v4.x ROC Template?

Refer to the following documents for details:

- *PCI DSS ROC Template Summary of Changes from ROC Template v4.0 to v4.0.1*.
- *PCI DSS v4.x ROC Template – Frequently Asked Questions r1* (for updates to the *PCI DSS v4.0 ROC Template).*

1.2 What are the options for implementing and validating requirements?

PCI DSS v4.x includes the following options for implementing and validating PCI DSS requirements:

ASSESSMENT APPROACH	WHEN TO USE THIS APPROACH
Customized Approach	Focuses on the Customized Approach Objective of each PCI DSS Requirement (if applicable), allowing entities to implement controls to meet the requirement's stated Customized Approach Objective in a way that does not strictly follow the defined requirement. The customized approach supports innovation in security practices, allowing entities greater flexibility to show how their current security controls meet PCI DSS requirements. Refer to the *PCI DSS Requirements and Testing Procedures v4.x* for the Customized Approach Objectives, included with each applicable requirement. ***Note:*** *If used by the assessed entity, the assessor completes and includes Appendix E Customized Approach Template with the ROC.* ***Note:*** *Compensating Controls are not an option for the Customized Approach*
Defined Approach	The traditional method for implementing and validating PCI DSS and uses the Requirements and Testing Procedures defined within the standard. The entity implements security controls to meet the stated requirements, and the assessor follows the defined testing procedures to verify that the requirement has been met. **Note on using Compensating Control(s)**: As part of the defined approach, entities that cannot meet a PCI DSS requirement explicitly as stated due to a legitimate and documented technical or business constraint may implement other or compensating controls that sufficiently mitigate the risk associated with the requirement. On an annual basis, any compensating controls must be documented by the entity and reviewed and validated by the assessor and included with the Report on Compliance submission. ***Note:*** *If used by the assessed entity, the assessor completes and includes Appendix C Compensating Controls Worksheet with the ROC.*

2. ROC Reporting Features for PCI DSS v4.x

2.1 What is the purpose of Section 1.7: Overall Assessment Result?

The *Overall Assessment Result* ROC section is to document the overall status of a PCI DSS assessment, based on findings noted in the *Assessment Findings* for each PCI DSS requirement. The *Overall Assessment Result* table below is excerpted from the *PCI DSS v4.x ROC Template*:

1.7 Overall Assessment Result

Indicate below whether a full or partial assessment was completed. Select only one.	
☐	**Full Assessment:** All requirements have been assessed and therefore no requirements were marked as Not Tested.
☐	**Partial Assessment:** One or more requirements have not been assessed and were therefore marked as Not Tested. Any requirement not assessed is noted as Not Tested in section 1.8.1 below.

Overall Assessment Result (Select only one)	
☐	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall COMPLIANT rating; thereby the assessed entity has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall NON-COMPLIANT rating; thereby the assessed entity has not demonstrated compliance with PCI DSS requirements.
☐	**Compliant but with Legal Exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall COMPLIANT BUT WITH LEGAL EXCEPTION rating, thereby the assessed entity has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.

2.2 In Part II: Section 7 Findings and Observations, what is the purpose of the Assessment Findings columns?

The *Assessment Findings* columns categorize the results of the assessment for each individual PCI DSS requirement.

These results are summarized in Section 1.8 *Summary of Assessment*.

Here is sample layout of Part II: Section 7 *Findings and Observations* that shows the headings and reporting options:

Requirement Description					
1.1 Example Requirement Description					
PCI DSS Requirement					
1.1.1 Example Requirement					
Assessment Findings (select one)				**Select If below Method(s) Was Used**	
In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Compensating Control***	**Customized Approach***
☐	☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.* **As applicable, complete and attach the corresponding documentation (Appendix C, Appendix E, or both) to support the method(s) used.*					
Testing Procedures	**Reporting Instructions**	**Reporting Details: Assessor's Response**			
1.1.1.a Example testing procedure	Example reporting instruction				
1.1.1.b Example testing procedure	Example reporting instruction				

2.3 What is the difference between the Overall Assessment Result in Section 1.7 and the Assessment Findings in Part II: Section 7 Findings and Observations?

The *Overall Assessment Result* in Section 1.7 of the ROC is a cumulative summary of all assessment findings, and is one of the following:

Overall Assessment Result
• Compliant • Compliant but with Legal Exception • Non-Compliant

The *Assessment Findings* in Part II shows the results for each individual PCI DSS requirement, and is one of the following:

Assessment Findings
• In Place • Not Applicable • Not Tested • Not in Place

2.4 For the sample layout shown in Q 2.2, for "Select If Below Method(s) Was Used," how does an assessor determine whether to select "Compensating Control" or "Customized Approach" for a requirement?

If an entity has implemented a compensating control to meet some or all aspects of a requirement, "Compensating Control" is selected. In this case, the assessor has performed expected testing of the compensating control and selects the corresponding Assessment Finding that accurately represents the results of the testing. The assessor also completes and includes the *Appendix C Compensating Controls Worksheet* in in the *PCI DSS v4.x ROC Template*.

See *PCI DSS v4.x Appendices B and C* for more details about compensating controls.

If an entity has implemented a customized approach to meet some or all aspects of a requirement, "Customized Approach" is selected. In this case, the assessor has derived appropriate testing procedures, performed testing of the customized control, and selects the corresponding Assessment Finding that accurately represents the results of the testing. The assessor also completes and includes the *Appendix E Customized Approach Template* in in the *PCI DSS v4.x ROC Template*. Note that compensating controls are not an option for meeting the same aspect of a requirement that is met with a customized approach.

See *PCI DSS v4.x Section 8*, and *PCI DSS v4.x Appendices D and E* for more details about the customized approach.

3. ROC Reporting Options for PCI DSS v4.x

3.1 What is the difference between the Full Assessment and Partial Assessment options in the ROC Template?

When an entity undergoes a Full Assessment, all PCI DSS requirements have been considered and no requirements are marked as Not Tested. When an entity undergoes a Partial Assessment, only a subset of PCI DSS requirements has been considered and one or more requirements are marked as Not Tested. Refer to question 4.2 below "What is the difference between Not Applicable and Not Tested?" for more information.

4. Assessment Findings

4.1 How does an assessor determine which assessment finding is appropriate when reporting results for a requirement?

The following table is a supplement to the explanation provided in the *ROC Template for PCI DSS v4.x*. Only one response should be selected for each sub-requirement.

Response	When to use this response:
In Place	The expected testing has been performed, and all elements of the requirement have been met.
Not Applicable (N/A)	The requirement does not apply to the organization's environment. Not Applicable responses require reporting on testing performed to confirm the Not Applicable status including a detailed description explaining how it was determined that the requirement does not apply. Note that reporting instructions that start with "If Yes" or "If No" do not require additional testing to confirm the Not Applicable status. For example, if the Reporting Instruction was "If Yes, complete the following" and the response was "No" then the assessor would simply mark that section as Not Applicable or N/A and no further testing is required.
Not Tested	The requirement (or any single aspect of the requirement) was not included for consideration in the assessment and was not tested in any way. (See "What is the difference between "Not Applicable" and "Not Tested"?" below at 4.2 for examples of when this option should be used.) ***Note**: Where Not Tested is used, the assessment is considered a Partial Assessment.*
Not in Place	Some or all elements of the requirement have not been met, are in the process of being implemented, or require further testing before it will be known if they are In Place. This response is also used if a requirement cannot be met due to a legal restriction, meaning that meeting the requirement would contravene a local or regional law or regulation. The assessor must confirm that a statutory law or regulation exists that prohibits the requirement from being met. ***Note:** Contractual obligations or legal advice are not legal restrictions*.

4.2 What is the difference between "Not Applicable" and "Not Tested?"

Requirements that are Not Applicable to an environment must be verified as such. Using the example of wireless and an organization that does not use wireless technology in any capacity, an assessor could select Not Applicable for Requirements 1.3.3, 2.3.1 - 2.3.3, and 4.2.1.2 after the assessor confirms through testing that there are no wireless technologies used in the organization's CDE or that connects to their CDE. Once this has been confirmed, the assessor may select Not Applicable for those specific requirements, and the accompanying reporting must reflect the testing performed to confirm the Not Applicable status.

If a requirement is completely excluded from review without any consideration as to whether it could apply, the Not Tested option must be selected. Examples of situations where this could occur may include:

- An organization may be asked by their acquirer or brand to validate a subset of requirements—for example, using the *PCI DSS Prioritized Approach* to address only certain milestones.
- An organization may want to validate a new security control that impacts only a subset of requirements—for example, implementation of a new encryption method that requires assessment of PCI DSS Requirements 2, 3, and 4.
- A service provider organization might offer a service that covers only a limited number of PCI DSS requirements—for example, a physical storage provider may want to validate only the physical security controls per PCI DSS Requirement 9 for their storage facility.

In these scenarios, the organization wants to validate only certain PCI DSS requirements, even though other requirements might also apply to their environment.

Items marked as Not Applicable require that the assessor render an opinion that the item is not applicable; however, with Not Tested, the assessor is simply following the entity's instructions to not test something with no opinion needed from the assessor.

The resulting ROC (in section 1.8.1) and AOC(s) (in Part 2g: Summary of Assessment) must indicate which if any requirements were Not Applicable or Not Tested.

The example below illustrates the difference between Not Applicable and Not Tested using different scenarios

	Not Applicable	Not Tested
Scenario	• A listed PCI SSC Validated P2PE solution is in place, *and* the entity fully meets all the eligibility criteria defined in SAQ P2PE • No CHD in the environment.	• A service provider organization offers a service that covers only a limited number of PCI DSS requirements-for example, a physical storage provider that wants to validate only the physical security controls per PCI DSS Requirement 9 for their storage facility. • Acquirer asks for a report only covering a subset of requirements (for example, using the PCI DSS Prioritized Approach).
Testing	Assessor performs the appropriate testing and validation on all requirements. Any PCI DSS requirement where testing verifies the non-applicability of that requirement is marked as **Not Applicable**, which would NOT result in a **Partial Assessment**.	Assessor performs appropriate testing and validation only for the specified requirements. The remaining requirements are marked as **Not Tested,** which would result in a **Partial Assessment.**

5. General Questions

5.1 Is use of the ROC Template for PCI DSS v4.x mandatory?

Yes. The PCI DSS ROC Template is mandatory for QSAs to use when documenting a detailed PCI DSS assessment (as contrasted with a less detailed PCI DSS self-assessment documented in a Self-Assessment Questionnaire (SAQ)). All response sections in the ROC Template must be completed (even if to note that sections or requirements are not applicable). Reporting requirements for ISAs should be discussed with the brands and/or acquirers to which the ROC will be submitted.

5.3 Where can I find the unlocked Microsoft Word version of the ROC Template for PCI DSS v4.x?

An up-to-date unlocked Microsoft Word version of the ROC Template for PCI DSS v4.x is available on the Assessor Portal (www.programs.pcissc.org) for assessors to download. Make sure to download a clean copy for each assessment, as there may be subsequent changes to the ROC Template for PCI DSS v4.x.

Contact your Program Manager directly if you cannot access the Assessor Portal. A PDF version of the ROC Template for PCI DSS v4.x is available on the PCI SSC website for non-assessor inquiries.

5.4 How should a QSA Company report typos or other errors in the ROC Template for PCI DSS v4.x?

Errors in the ROC Template for PCI DSS v4.x should be reported to the Program Manager. Please include all relevant details regarding the error such as operating system and word processor used when experiencing the error.

5.4 Can a QSA company make personalization-type changes to the ROC Template for PCI DSS v4.x and, if so, what are the limitations?

A QSA Company may want to make personalization changes to the *ROC Template for PCI DSS v4.x*, such as the addition of company logos and addition of legal verbiage. For this reason, a customizable title page has been added to the *ROC Template for PCI DSS v4.x*. Personalization must be limited to the customizable title page and the headers of the remainder of the document. The addition of table rows is permitted as needed throughout the document. The assessor may optionally delete PCI SSC cover page for the *ROC Template*, the *Document Changes* table, the *ROC Template Table of Contents*, and the *ROC Template Instructions* prior to submitting the final report to the customer. The addition of content, such as legal verbiage, is allowed and must be limited to the customizable title page.

Other changes must be minimal and the format of the *ROC Template for PCI DSS v4.x* must remain unchanged. This includes reordering of sections, which is NOT allowed. Nothing is permitted to be removed from Parts I and II of the document, including sections or requirements determined to be not applicable. Those sections and/or requirements must remain in the completed ROC Template with the “Not Applicable” result documented instead. Edits to the footers are explicitly not allowed.

The following changes are **permitted**:

- Addition of Company logos and legal verbiage
- Changes to the customizable title page
- Changes to the page headers
- Additions of table rows
- Removal of the *ROC Template* PCI SSC cover page, the *Document Changes* table, the *ROC Template Table of Contents*, and ROC Template Instructions

The following changes are **prohibited**:

- Edits to the footers
- Changes to the format of the *ROC Template for PCI DSS v4.x*
- Reordering or removal of sections or requirements
- Removal of any content from Parts I and II including reporting instructions in those sections

The following should be **considered** when making changes:

- Ensure that any content added by the QSA is clearly distinguishable from the content that is part of the published PCI SSC document. All additions should be considered carefully, and such content should be added only to the customizable title page of the document.
- The entities to which a ROC is submitted (payment brands and/or acquirers) may choose not to accept any report that has changes to the ROC Template they believe are unacceptable.

5.5 Can a QSA Company use a reporting tool to generate a ROC (for example, a PDF generated from HTML)?

Yes, but with the understanding that the product of any reporting tool must include all content from, and mirror, the PCI DSS ROC Template. If a reporting tool does do that, QSAs must report directly into the ROC Template Word file.

5.6 Do ROCs and ROVs need to be completed only in English or may they be produced in the local language?

PCI SSC does not require that the ROC be completed in English; however, the QSA will be required to translate to English at their own expense if PCI SSC requests reports, work papers, etc. at any point. Check with the brands/acquirers to which the ROC will be submitted as to their language requirements.

5.7 Will PCI SSC be translating the PCI DSS v4.x ROC Template into other languages? May I translate the document myself?

PCI SSC only provides the PCI DSS v4.x ROC Template in English. However, it is recognized that not all work is done in English and that translations may be necessary. If a QSA translates this document, PCI SSC requires the following:

- QSA must provide both PCI SSC's English version and QSA's translated version to customers/end-users, noting that the English version from PCI SSC governs in the event of any conflict.
- After the table of contents at the beginning of the document, the following disclaimer must be included in both in English and the translated language: "Note – This document (the "Translation") is an unofficial, <<final language>> language translation of the original English language version provided herewith ("Official Version"). The Translation has been prepared by <<QSA Company>>, and PCI SSC has not had any involvement in and does not endorse the Translation. <QSA Company> hereby certifies that it has made all attempts to ensure that the Translation accurately, completely, and truly reflects the Official Version in form and substance. <<QSA Company>> is and shall be solely responsible for any and all liability resulting from any error in translation or inconsistency between the Official Version and the Translation."

5.8 Have requirements for work papers and retention of work papers changed?

No. Requirements for generation and retention of work papers have not changed. Refer to the current version of *QSA Program Guide* for expectations regarding work papers and evidence. Assessors are expected to collect evidence to support the contents of the ROC from end-to-end. As explained in the "ROC Template Instructions" section of the ROC Template for PCI DSS v4.x, work papers contain comprehensive records of the assessment activities including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during an assessment to support the assessor's findings.

5.9 When a QSA Company is audited, are the audits conducted using reports from only the most recent standard?

Any audits will continue to employ a sampling of completed reports, which could include v3.2.1 and v4.x reporting. It is important to continue to strive for quality reporting when assessing against either standard, and the expectations around 3.2.1 have not changed. Assessors should be prepared to be audited for any work they've completed, including reporting, work papers, and similar. The company will receive feedback no matter what version of reporting is used.

5.10 Are requirements noted as "best practice until 31 March 2025" considered "Not Applicable" or "Not Tested"?

Requirements noted as best practices until 31 March 2025 are not required to be tested until that date has passed. As such, a "Not Applicable" response to future-dated requirements is accurate.

Once the future date has passed, responses to those requirements should be consistent with instructions for all requirements.

Note – Requirements that are future-dated are considered as best practices until the future date is reached. During this time, organizations are not required to validate to future-dated requirements. While validation is not required, organizations that have implemented controls to meet the new requirements and are ready to have the controls assessed prior to the stated future date are encouraged to do so. Once the designated future date is reached, all future-dated requirements become effective and applicable.

6. Account data storage

6.1 My client feels that the Storage of Account Data table in the completed ROC combines a lot of sensitive data into one document. How can I address their concerns, but complete the ROC Template appropriately?

It is acceptable in the ROC Template at 4.3 for the QSA to attest that the storage of account data has been separately documented according to 4.3 and to include a document reference to identify where in the work papers it can be found. PCI SSC reserves the right to request any work papers and may request this to ensure that the required details are recorded. Like all work papers, this must be retained by the QSA pursuant to the QSA Agreement.

7. AOC

7.1 Regarding the AOC for Service Providers, are formal definitions provided for the services listed?

PCI SSC does not provide formal definitions for these services. As noted in Part 2 of the AOC for Service Providers, v4.x: *"Note: These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories don't apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with entity(ies) to which this AOC will be submitted."*