Payment Card Industry

Data Security Standard

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

March 2022

Purpose of document

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

1. Overview of PCI DSS v4.x Reporting

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

ROC Section	Description of Change
Throughout	Updates to reflect changes in PCI DSS v4.x
	Updates to improve clarity and reduce redundancy
	Separated the ROC into three parts: 1. ROC Template Instructions – instructional content that is used to complete the ROC. This part can optionally be deleted prior to releasing the final report 2. Part I: Assessment Overview 3. Part II: Findings and Observations and Appendices In parts I and II minor modifications are allowed, such as increasing/decreasing the number of rows or to change the column width; however, deletion of content is not allowed.
	Use of reference numbers in the Summary Overview/Findings and Observations is no longer optional. There is also the option to identify items in the response in the Findings and Observations section in addition to the reference number.
	Updated Summary of Assessment Findings (aligns with new checkboxes within the Findings and Observations) 1. Added “In Place with Remediation” 2. Deleted “In Place w/ CCW” (instead, reporting for Compensating Controls is captured in the “Validation Method” section for each sub-requirement)
ROC Template Instructions	Added Assessment Findings table indicating when each finding is to be used and what reporting is required
	Added Instructions for Assessment Approach Reporting Options

ROC Section	Description of Change
	Aligned the Reporting Instruction Terms for consistency with other PCI standards: 1. Indicate 2. Identify 3. Describe 4. Attest
Part I: Assessment Overview	Added a customizable title page
	Updated the Overall Assessment Results to align with the AOC 1. Full/Partial Assessment 1. Indicate whether a Full Assessment or a Partial Assessment was completed. 2. Overall Assessment Result (Same three options exist in the AOC of PCI DSS v3.2.1) 1. Compliant 2. Compliant but with Legal Exception 3. Not Compliant
	Added following sections: 1. Remote Assessment Activities 2. Use of Subcontractors 3. Additional Information/Reporting 4. Overall Assessment Result 5. Attestation Signatures 6. Storage of SAD 7. Quarterly Internal Scan Results
	Added Section 6 Evidence (Assessment Workpapers)
	Removed sections including: 1. PCI DSS version 2. Connected entities for payment processing and transmission 3. Other business entities that require compliance with the PCI DSS 4. Wireless summary 5. Managed service providers
	Updated, merged, and/or moved sections to reduce redundancy, add clarity, and/or improve readability

ROC Section	Description of Change
Part II: Findings and Observations	Reporting updated to facilitate reporting for defined approach, customized approach, or a combination of the two
	Updated the reporting to focus more on referencing evidence for the defined approach
	Added a narrative for each requirement to explain why the assessment finding was selected. Specific instructions for each assessment finding are found in the "Required Reporting" column in the Assessment Findings section in ROC Template Instructions
Appendices	Minor updates to Compensating Controls Worksheet
	Addition of Customized Approach 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 (New option)	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 v4.0* for the Customized Approach Objectives, included with each applicable requirement. ***Note:*** *Compensating Controls are not an option for the Customized Approach*
Defined Approach (Existing 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.

2. New ROC Reporting Features for PCI DSS v4.x

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

Overall Assessment Result is a new ROC section to provide 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 1) In Place, 2) In Place with Remediation, or 3) 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 1) In Place, 2) In

2.2 In Part II: 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. ***Note*** *that this is not a new section of the ROC, but it does include a new reporting option.*

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

Here is an excerpt from Part II: *Findings and Observations* that shows the headings and reporting options:

Requirement Description				
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.				
PCI DSS Requirement				
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.				
Assessment Findings (select one)				
In Place	**In Place with Remediation**	**Not Applicable**	**Not Tested**	**Not in Place**
☐	☐	☐	☐	☐
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.*			<Enter Response Here>	

2.3 What is the difference between the Overall Assessment Result in Section 1.7 and the Assessment Findings in Part II: 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	
1.	Compliant
2.	Compliant but with Legal Exception
3.	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	
1.	In Place
2.	In Place with Remediation
3.	Not Applicable
4.	Not Tested
5.	Not in Place

2.4 What is the purpose of section 1.9 Attestation Signatures?

The attestation signatures section is intended to emphasize to the assessor the importance of conducting an independent, fact-based assessment that is complete and accurate to the best of the assessor's knowledge and to capture such acknowledgement by the assessor for PCI SSC quality assurance purposes. This section does not change the intended audience or distribution methods for the ROC.

3. New ROC Reporting Options for PCI DSS v4.x Explained

3.1 Why have Full Assessment and Partial Assessment been added to the ROC Template?

These reporting options have been added to provide better transparency in reporting. 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.

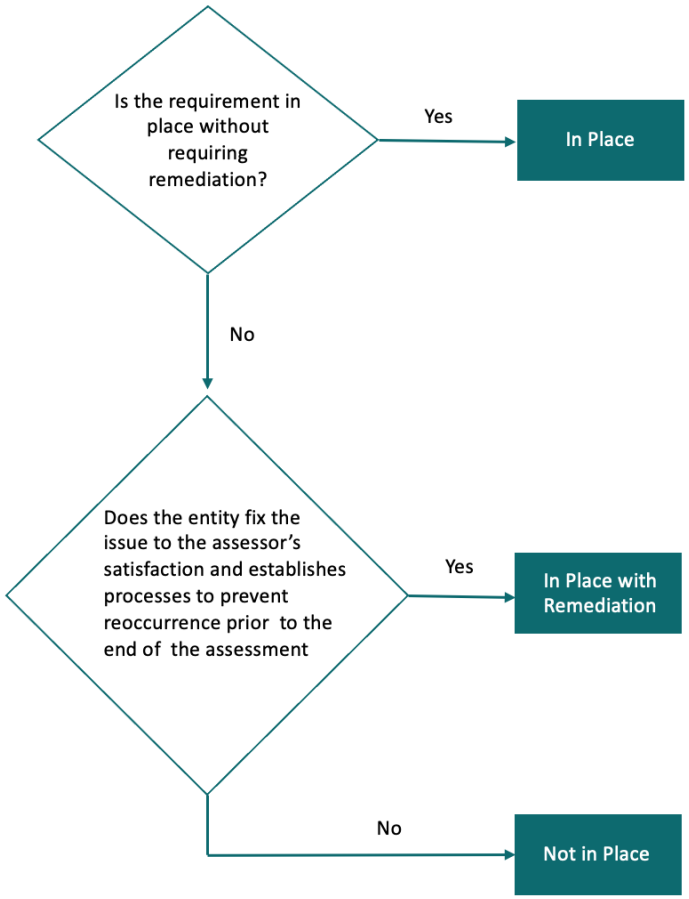
3.2 What is the purpose of In Place with Remediation in Assessment Findings?

In Place with Remediation is used when a requirement was not in place at some point during the PCI DSS assessment period, but where the entity remediated the issue such that the requirement was in place before the completion of the assessment. This option provides reporting transparency so that report reviewers can better understand the entity's security posture throughout the assessment period.

In Place with Remediation is recorded in the *Assessment Findings* section of the ROC and is a Compliant result in the *Overall Assessment Result* section of the ROC. In all cases where In Place with Remediation is used, the assessor must have assurance that the entity has identified and addressed the reason why the control failed, has implemented the control, and has implemented ongoing processes to prevent re-occurrence of the control failure.

An example of the use of In Place with Remediation is when an entity cannot provide evidence that ASV scans were conducted every quarter during the past year, but where the entity conducts the ASV scan, determined why scans were missed in the past, and implements processes to prevent re-occurrence in the future. Other examples include:

- A security patch that was not applied within 30 days.
- A misconfigured network security control.
- A missing or inadequate policy document.
- Unintentional storage of unencrypted PAN.
- Unintentional storage of SAD.



3.3 Can an Assessment Finding be noted as In Place with Remediation if the entity has not addressed the underlying issue?

No. An *Assessment Finding* can only be noted as In Place with Remediation if, before the end of the assessment, the entity has addressed the issue and implemented ongoing processes to prevent its re-occurrence.

4. Assessment Findings

4.1 When determining which one of the summary findings is appropriate for a sub-requirement, is there any more guidance available on those options beyond what is in the "Introduction to the ROC Template" section of the ROC Template for PCI DSS v4.x?

The following table is a supplement to the explanation provided within the ROC Template for PCI DSS v4.x. Only one response should be selected at the 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.
In Place with Remediation	The requirement was Not in Place at some point during the PCI DSS assessment period, but where the entity remediated the issue such that the requirement was In Place before completion of the assessment. In all cases of In Place with Remediation, the assessor must have assurance that the entity has identified and addressed the reason that the control failed, has implemented the control, and has implemented ongoing processes to prevent re-occurrence of the control failure.
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 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 connect 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 prioritized approach to validate 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 only to validate the physical security controls per PCI DSS Requirement 9 for their storage facility.

In these scenarios, the organization wants only to validate certain PCI DSS requirements, even though other requirements might also apply to their environment. The resulting AOC(s) must be clear in what was tested and not tested.

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 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 only wishes to validate the physical security controls per PCI DSS Requirement 9 for their storage facility. • Acquirer asking for a report on a subset of requirements (for example, the 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 result in a **Full Assessment***. *By definition, no requirements are marked as "Not Tested".	Assessor only validates the physical security controls per PCI DSS Requirement 9. 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?

The PCI DSS ROC Template is mandatory for QSAs to use for official reporting of a PCI DSS assessment. Requirements for ISAs and reporting should be discussed with the brands and/or acquirers accepting the Report on Compliance. For official reporting of a PCI DSS v4.0 assessment by a QSA, the ROC Template must be completed, with all response sections completed (even if to note that sections or requirements are not applicable).

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

The most 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. Please be sure to download a clean copy before each assessment, as there may be subsequent changes to the ROC Template for PCI DSS v4.x during the PCI DSS v4 lifecycle.

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.

5.3 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?

PCI SSC recognizes the need for personalization changes by the QSA to the ROC Template for PCI DSS v4.x, such as the addition of company logos and addition of legal verbiage. Therefore, 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 *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 shall 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 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:

- QSAs must ensure there is reasonable distinction between the content has been added by the QSA and is not 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.
- Accepting entities (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 our company use our reporting tool to generate the report (such as a PDF generated from HTML), provided that the look and the content closely follow the original?

PCI SSC will allow this, but with the understanding that what your reporting tool produces must include all content from the Reporting Template and look just like the PCI SSC Reporting Template. If it cannot do that, do not use the tool and report directly into the Word file.

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

There is not a PCI SSC requirement that the ROC be compiled 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 accepting brands/acquirers 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?

Requirements for work papers and retention of work papers have not changed; however, please review the current version of QSA Program Guide for expectations regarding 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 the course of the 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. Cardholder data storage

6.1 My client feels that inclusion of the cardholder data storage table in the completed ROC puts too much sensitive data into one document. How can I address their concerns, but complete the ROC Template appropriately?

In this case, it may make sense to put a document reference in the ROC Template at 4.3 for the QSA to attest that the cardholder data storage has been documented according to 4.3 and 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 would need to be retained by the QSA pursuant to the QSA Agreement.

7. AOC

7.1 Regarding the AOC for Service Providers, v4.x, are you planning to issue definitions for the services listed or similar guidance?

PCI SSC does not plan to 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 you feel these categories don’t apply to your service, complete “Others.” If you’re unsure whether a category could apply to your service, consult with the applicable payment brand.”