Payment Card Industry (PCI)
Data Security Standard

Frequently Asked Questions for use with ROC Reporting Template for PCI DSS v3.x

April 2015

ROC Reporting Template for PCI DSS v3.x: Frequently Asked Questions (FAQs)

Purpose of document

This document addresses questions around the use of the ROC Reporting Template for PCI DSS v3.x *(PCI Template for Report on Compliance, for use with PCI DSS v3.0 and subsequent versions against 3.x)*.

General Questions

Q 1 Is use of the ROC Reporting Template for PCI DSS v3.x mandatory?

A *The ROC Reporting Template for PCI DSS v3.x is mandatory for use by QSAs assessing against PCI DSS v3.x. Requirements for ISAs and reporting should be discussed with the brands and/or acquirers accepting the Report on Compliance. An assessment against v3.x of the PCI DSS by a QSA must be completed using this Reporting Template, with all grey boxes and response sections completed (even if to note it is not applicable).*

Q 2 I'm confused about when to use which document versions and how to pair them up. Please explain it as simply as possible.

A *When you assess against 3.x, you need to use the Reporting Template for 3.x, the version 3.x Attestations and the other supporting 3.x documents.*

Q 3 Where can I find the unlocked Microsoft Word version of the ROC Reporting Template for PCI DSS v3.x?

A *The most up-to-date unlocked Microsoft Word version of the ROC Reporting Template for PCI DSS v3.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 Reporting Template for PCI DSS v3.x during the PCI DSS v3 lifecycle.*

Contact your Program Manager directly if you cannot access the Assessor Portal. A PDF version of the ROC Reporting Template for PCI DSS v3 is available on the PCI SSC website for non-assessor inquiries.

Q 4 Can a QSA company make personalization-type changes to the ROC Reporting Template for PCI DSS v3.x and, if so, what are the limitations?

A *PCI SSC recognizes the need for personalization changes by the QSA to the ROC Reporting Template for PCI DSS v3.x, such as the addition of company logos (preferably limited to the title page) and addition of legal verbiage. Changes must be minimal and the format of the ROC Reporting Template for PCI DSS v3.x must remain unchanged. This includes reordering of sections, which is NOT allowed. Generally, changes to the format should be limited to the addition of rows as needed. Nothing is permitted to be removed, including sections or requirements determined to be not applicable. Those sections and/or requirements shall remain in the completed ROC Reporting Template with the "not applicable" result documented instead.*

The addition of content, such as legal verbiage, is allowed. PCI SSC would request that QSAs ensure there is reasonable distinction that the content has been added by the QSA and is not part of the published PCI SSC document. PCI SSC would also advise that such additions be

considered carefully and such content should be added in the form of addendums to the document, with references to the addendum places with the report.

Accepting entities (Payment Brands and/or Acquirers) may choose not to accept any report that has changes to the ROC Reporting Template they believe are unacceptable.

Q 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?

A *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.*

Q 6 Before I give the final report to my client, can I remove the instruction column? I want it to look as professional as possible.

A *Do not remove any column from the report, particularly this column. The premise of allowing QSAs to provide these sorts of answers is based on the context the instructions in that column provide. Without the column, the responses are not worth much and really would not make sense. Assessor Quality Management (AQM) believes that your client will see the most value in a report that is thorough and specific to them. We believe this Reporting Template can provide that and have created it with their needs in mind. However, if you receive any feedback from your clients, we invite you to forward it to the Program Managers so we may consider it for future changes.*

Q 7 Do ROCs and ROVs need to be compiled only in English or may they be produced in the local language?

A *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.*

Q 8 Into what other languages will the ROC Reporting Template for PCI DSS v3.x be translated by PCI SSC? May I translate the document myself?

A *There are no plans at this time for PCI SSC to translate the ROC Reporting Template for PCI DSS v3.x into any language other than 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:*

1. *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.*
2. *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."*

Q 9 What happened to the Reporting Methodology instructions and checkmarks that were in the Reporting Instructions for PCI DSS v2.0, but appear to be missing from the ROC Reporting Template for PCI DSS v3.x?

A *PCI SSC removed the Reporting Methodology instructions and checkmark columns after determining they were no longer necessary for ROC Reporting Template for PCI DSS v3.x due to the extensive changes that were made between the Reporting Instructions for 2.0 and the Reporting Template for 3.0.*

The Reporting Instructions within the ROC Reporting Template for PCI DSS v3.x, in support of the enhanced Testing Requirements in PCI DSS v3.x, are explicit in what methodology is expected to be in use. By including a more precise Reporting Instruction directly in the Reporting Template next to the Testing Procedure, expectations regarding methodologies used to complete tests required are self-evident.

Q 10 Have requirements for work papers and retention of work papers changed?

A *Requirements for work papers and retention of work papers have not changed. Assessors are expected to collect evidence to support all findings. As explained in the "Assessor Documentation" section of the Reporting Instructions for PCI DSS v2.0 and in the "Introduction to the ROC Template" section of the ROC Reporting Template for PCI DSS v3.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.*

Q 11 How do we ensure that we don't "repeat or echo the Testing Procedure in the response," when the responses relate directly to the testing procedures?

A *With the ROC Reporting Template for PCI DSS v3.x, the Reporting Instruction is present directly next to the QSA's response field, and that instruction already essentially repeats or echoes the content of the Testing Procedure. There is no need to repeat it once more, and doing so provides none of the assurance that the assessor's reporting should provide. Instead, assessors are expected to provide detail specific to the individual assessment regarding how they verified that a requirement is met. The detail of the response should be sufficient to support the conclusion and provide assurance as to* ***how*** *the Requirement was verified, not just that it was verified.*

ROC Section and PCI DSS Testing Procedure Questions

Assessor Validation of Scope Accuracy

Q 12 The instructions for "3.1 Assessor's validation of scope accuracy" seem inconsistent with the critical distinction that PCI DSS establishes, which is that scope definition is the responsibility of the entity, and that the assessor verifies that the scope was defined properly. Has that changed?

A *It is true that the assessor is tasked with verifying the scope has been defined properly, and that the scope definition in many cases is set by the assessed entity separate from the assessor. No matter who defined the scope, however, it is important for the assessor to understand how it was determined and document those findings. As such, it may be that the response at the first bullet, for example, regarding the methods or processes used to identify and document all existences of cardholder data, includes a response by the assessor that states that the assessed entity used X, Y, and Z methods and processes to identify and document all existences of cardholder data.*

The results of that, the bullet where the instruction is to describe "how the results of the methods/processes were documented" may include details not of what the assessor did, but what the assessor determined the entity did, such as a resulting inventory of cardholder data locations. The assessor is verifying and reporting on how these were done—whether by the assessor or entity—but the assessor's own actions and judgment may be limited to "Why the methods used for scope verification are considered by the assessor to be effective and accurate," and the assessor attestation stating "that the scope of the assessment has been verified to be accurate and appropriate."

Q 13 How does using a PA-DSS validated application affect the scope of a merchant's PCI DSS assessment?

A *Applications that are PA-DSS validated have been assessed by a PA-QSA as meeting all PA-DSS requirements. This means the application, when properly installed and configured in the cardholder data environment, is capable of supporting the merchant's PCI DSS compliance.*

Using a PA-DSS validated application does not reduce the scope of the merchant's cardholder data environment; the boundaries of the cardholder data environment remain unchanged and the application must be included in the PCI DSS assessment of the merchant's environment. As part of the PCI DSS assessment the assessor must verify that the application has been appropriately implemented and configured.

Sampling

Q 14 Where a testing procedure includes sampling of system components, should a list of host names or IP addresses be included in the response?

A *As explained in the "ROC Reporting Details" section, the assessor should identify the number and type of items included in each sample. It is not necessary to identify or name every sampled system component in the ROC; however, assessors may provide a list if it improves clarity or better explains the findings for some environments.*

Irrespective of whether system component names are recorded in the ROC, the assessor must maintain a detailed record of each sampled component in their work papers, and provide full details of their sampling methodology in Section 3 of the ROC, "Description of Scope of Work and Approach Taken."

Q 15 How will the "appropriateness" of a sample be measured?

A *The details required in Section 3 of the ROC, "Description of Scope of Work and Approach Taken," provide the assessor's justification of why the samples chosen are appropriate.*

Details about Reviewed Environment

Q 16 Is a complete itemized list of every hardware device, either by IP address or hostname, required for the "List of Hardware" in the "Details about Reviewed Environment" section of the ROC?

A *A list detailing every individual IP address and/or hostname is not required for the ROC. The List of Hardware should identify each type of hardware used in the cardholder data environment as defined in the "ROC Reporting Details" column. However, assessors are expected to maintain a more detailed list as part of their work papers.*

Cardholder data storage

Q 17 My client does not want to have the cardholder data storage table included in the completed ROC, as they feel it puts too much secure data into one document. How can I address their concerns, but complete the ROC Template appropriately?

A *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.*

Summary of Result Findings

Q 18 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 Reporting Template for PCI DSS v3.x?

A *The following table is a helpful supplement to the explanation provided within the ROC Reporting Template for PCI DSS v3.x. Remember, 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 as stated.
In Place w/ CCW (Compensating Control Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Control Worksheet (CCW) Information on the use of compensating controls and guidance on how to complete the worksheet is provided in the PCI DSS.
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
N/A (Not Applicable)	The requirement does not apply to the organization's environment. All "not applicable" responses require reporting on testing performed to confirm the "not applicable" status.
Not Tested	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 Q19 for examples of when this option should be used.)

Q 19 What is the difference between "Not Applicable" and "Not Tested"?

A *Requirements that are deemed to be 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 "N/A" for Requirements 1.2.3, 2.1.1, and 4.1.1, after the assessor confirms that there are no wireless technologies used in their CDE or that connect to their CDE via assessor testing. Once this has been confirmed, the organization may select "N/A" 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 should be selected. Examples of situations where this could occur may include:

- *An organization may be asked by their acquirer to validate a subset of requirements—for example: using the prioritized approach to validate certain milestones.*
- *An organization may wish to validate a new security control that impacts only a subset of requirements—for example, implementation of a new encryption methodology 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 only wish to validate the physical security controls per PCI DSS Requirement 9 for their storage facility.*

In these scenarios, the organization only wishes to validate certain PCI DSS requirements even though other requirements might also apply to their environment. Compliance is determined by the brands and acquirers, and the AOCs they see will be clear in what was tested and not tested. They will decide whether to accept a ROC with something "not tested," and the QSA should speak with them if any exception like this is planned. This should not change current practice, just reporting.

Q 20 Can you clarify the difference in "Not Applicable" versus "Not Tested" for a scenario such as a cloud services (Infrastructure as a Service) provider? In that case, the service provider would not be responsible for applications or other aspects that the customer is responsible for. Are those N/A or not tested?

First, consider the guidance that if a requirement was considered and tested to confirm it is not applicable, it is "not applicable." If the requirement is excluded from review and/or testing without any consideration and/or testing as to whether it could apply to this assessment, the "Not Tested" option is appropriate. A "not applicable" response still requires a level of testing, and that should be evident in the designation and the accompanying reporting response. From there you look at these specific scenarios.

In the specific example of a cloud services provider who offers infrastructure as a service and is not responsible for applications or other aspects that the customer is responsible for, the determination as to whether "not applicable" or "not tested" is most appropriate is a decision for the assessor and accepting entity, with a few considerations. The assessor should review legal agreements and/or other documented evidence that defines who has what responsibility. If these support that these are not the responsibility of the service provider, then "not applicable" could be appropriate (and the review of that documented evidence can be considered the testing mentioned above). If there is not sufficient evidence or perhaps the service provider has not identified those services in scope of the assessment, "not tested" may be appropriate and will allow the transparency intended here for any customers depending on the compliance of this service provider. Part of the intent of the "not tested" option is to clearly demonstrate that such aspects were excluded from testing and/or scope so that merchants using the services of the service provider don't make assumptions as to the level of testing and so that service providers (or any assessed entity using the "not tested" option) do not misrepresent their compliance efforts.

Beyond the specific scenario above, where I am a large entity with many offerings but I am only validating for a single service offering or a defined subset of service offerings, then those requirements not included in scope are "not tested." Those offerings aren't in scope of the current assessment and a "not tested" response should allow the scope and requirements tested in the AOC/ROC to reflect obligations to such an entity's clients. This is where it is also important for the assessor to ensure the scope of the investigation is accurate and appropriate; if the AOC/ROC is to represent just the cloud service offering, the scope and resulting AOC/ROC should make sense. It isn't that they don't exist or don't apply to the environment, but they aren't being tested for the sake of this assessment.

There is a difference between an entity being assessed and relying on another entity's PCI compliance for requirements (confirmed via contracts) and an entity being assessed and not having contracted responsibility for certain requirements because they are deemed the

responsibility of the client (again, confirmed via contracts). In most likelihood, if the entity being assessed doesn't have contracted responsibility for certain requirements and for that reason is not demonstrating compliance at those requirements, a "Not Tested" is appropriate. See the below note for the entity with contracted or otherwise designated responsibility.

***Note**: The March 2014 version of this FAQ noted the following example for "Not Applicable" in error; dependence on other entity's PCI Compliance is deemed "In Place" with a narrative similar to the below reflecting review of the contract and confirmation of PCI Compliance via review of the corresponding AOC. On the other side of this, if I use a hosting provider and my compliance for some requirements is based on their PCI compliance, there is still some testing—in that the QSA will still ensure contracts reflect that responsibility, the ROC or AOC will be reviewed to ensure it covers this responsibility—and the "In Place" response will reflect that testing. You might end up with a response like "In Place. QSA confirmed contract dated xx/xx notes this as responsibility of SP Y. Reviewed AOC of SP Y, confirmed they are PCI Compliant against 2.0 as of yy/yy."*

Q 21 Are future-dated requirements considered "Not Applicable" or "Not Tested"? The instructions in the ROC Reporting Template for PCI DSS v3.0 seem to conflict on this.

A *An update to the ROC Reporting Template for PCI DSS v3.0 has clarified this, as the original instructions have been determined to not reflect effectively the result. While it is true that the requirement is likely not tested (hence the original instructions), it is not required to be tested until the future date has passed, and the requirement is therefore not applicable until that date. As such, a "Not Applicable" response to future-dated requirements is accurate, whereas a "Not Tested" response would imply there was not any consideration as to whether it could apply (and be perceived as a partial or incomplete ROC).*

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

Q 22 There appear to be several typos or issues with instructions in a couple places. Are there plans to remedy these soon and what do we do in the meantime?

A *AQM has published an updated version of the 3.0 templates to the Portal, as was always the intention, and will continue to publish subsequent revisions. It was a large endeavor to create these documents, and despite our best efforts, we knew some corrections would need to be made. Some are simply mistakes, such as the example of 6.4.4.b and 8.7.b in the Reporting Template for 3.0, version 1.0 where the wrong word appears in the instruction. As mentioned before, the intent for how to handle future-dated requirements as "not applicable" was a change made after publication and that needs to be remedied. Please continue to send such feedback to the Program Managers so we may fix it, and look forward to these published updates. In the meantime, ensure your response addresses the intent clearly.*

Q 23 I am curious why the "N/A" is grayed out for 3.2.1. I can see situations (physical security facility) that might look at this question as N/A since the client would be responsible for the application and database.

A *There is not a change in intent here, and was addressed in the August 2011 Assessor Update Newsletter. Some of the highlights follow, but please refer back to that publication:*

Checking for SAD – PCI DSS and PA-DSS

Regarding the testing procedures found in PCI DSS Requirements 3.2.1 – 3.2.3 and PA-DSS Requirements 1.1.1 – 1.1.3, these testing procedure responses can never be "Not Applicable." These requirements are a fundamental part of the Standards and each review must fully account for all Sensitive Authentication Data (SAD) that may enter the assessed environment or application.

SAD could be lurking anywhere, and an exhaustive investigation into all applicable storage areas and storage types is necessary. All payment application output needs to be examined to ensure that SAD isn't being unknowingly propagated to areas outside of the application. As the expert on the ground, it is the responsibility of the assessor to look for all possible instances of Sensitive Authentication Data, even in areas that may be unknown to your client.

Q 24 What is the intent of having the QSA name in several sections of the report within the requirements, such as the "Provide the name of the assessor who confirms that…" instructions?

A *AQM gave each response instruction close consideration and did not want to encourage reporting for the sake of reporting. In most places, there were details the assessor could provide that would not boil down to "yes/no" or repeating of the testing procedure, but that was not the case for all. In the requirements where it was determined that no additional useful reporting was likely, we determined this "signature" was a better course of action. The consistency of using the assessor's name as an attestation is deemed stronger than a simple "yes" or "checkmark."*

Q 25 If my company is audited in 2014, will we be audited using reports against 2.0, 3.x, or both?

A *Any audits will continue to employ a sampling of completed reports, which could include both 2.0 and 3.x reporting. It is important to continue to strive for quality reporting when assessing against both standards, and the expectations around 2.0 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.*

Q 26 My company has already begun assessing against 3.x and we've come up with a report. Can AQM or someone at the PCI SSC take a look at it and tell me if the reporting is acceptable?

A *Consulting is not an offering that AQM or PCI SSC can provide at this time, so we are not able to take requests for this sort of work. We invite you and your QA personnel to consider whether responses answer the questions they are supposed to and provide a level of detail that supports assurance of quality assessment via quality reporting. If you aim to be as generic as possible to repeat language through reports, you are unlikely to achieve that. If you answer specific to the one client and provide meaningful detail, even if brief, you are on the right track.*

Attestation of Compliance (AOC)

Q 27 The AOC for merchants has no mention of which or how many requirements were "not tested." Why? Doesn't this mean that a merchant can "not test" many items and not make it clear as to how thorough their assessment was?

A *Because the compliance of entities are often dependent on the compliance of service providers, there was a clear need to provide more information within the AOC for Service Providers regarding which requirements were not tested, etc., based on the feedback we received from the community. Merchants, however, are less likely to be taking on responsibility for requirements for entities in this manner, and therefore this level of reporting isn't necessary in the AOC for Merchants. Remember, compliance is determined by the brands and acquirers, and any intention to not test requirements should be discussed with them. The addition of "Not Tested" is not intended to make requirements optional, but to facilitate reporting of partial assessments and the like.*

Q 28 Regarding the AOC for Service Providers, v3.x, are you planning to issue definitions for the services listed or similar guidance?

A *There are no plans at this time for formal definitions for these services by PCI SSC. As noted in Part 2 of the AOC for Service Providers, v3.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."*