ROC Reporting Instructions for PCI DSS v2.0
Frequently Asked Questions (FAQs)

Purpose of document

This document addresses questions around the use of the ROC Reporting Instructions for PCI DSS v2.0.

General Questions

Q 1  Is the assessor expected to collect physical evidence for “Interviews with personnel” or “Observe process, action, state” reporting methods?
   A  Assessors are expected to collect evidence to support all findings. As explained in the “Assessor Documentation” section, 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 2  Are the items listed under each “Example Instruction” in the “ROC Reporting Details” section (pages 8 and 9) always required for that instruction?
   A  The details in this section provide guidance to assist in understanding the reporting details. Not all items may be required for every response. The assessor is expected to be able to determine what is applicable for the particular environment they are assessing.

Q 3  Can observations covering two or more reporting methods (for example, “Observe system settings, configuration” and “Observe process, action, state”) be recorded in one statement or should they be separated into multiple statements?
   A  Observations that cover more than one reporting methodology may be combined into one statement as long as it is clear to the reader what methods were performed and the associated results. The quality of a response is determined by the inclusion of all relevant information, not the number of statements.

Q 4  The instructions include, “Don’t copy responses from previous assessments.” What happens if our findings are the same for a particular entity from one year to the next?
   A  Assessors are expected to perform a fresh assessment each year, as the results from previous years are not necessarily relevant for a current assessment. Where a finding happens to be the same from one year to the next, the details provided in the ROC may be similar but they should not be duplicates. Each requirement should be reviewed against the current environment such that the assessment findings are current and independent of previous years’ assessments.

Q 5  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  Assessors are expected to explain how they verified that a requirement is met, and not simply respond with “The assessor verified that <paste requirement here> is in place.” Breaking down the response into specific details should help the assessor think about how they validated a requirement, rather than simply stating that they did.
Q 6  I’m not sure whether an instruction “Describe how the observed system...” refers to the check mark (✓) under “Observe system, setting, configuration” or “Observe process, action, state.” How can I be sure which one to report?

A  Observations of a system “state” may include elements of system configuration or system settings. If there is an overlap, don’t be concerned which “Reporting Methodology” column the check mark is located in; instead, focus on understanding the response as described in the “Reporting Details” column and clearly describing what was in fact observed.

ROC Section and PCI DSS Testing Procedure Questions

Sampling

Q 7  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 (page 9), 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 the “Description of Scope of Work and Approach Taken” section of the ROC.

Q 8  Should the number of devices sampled be included just in the executive summary, or for every response relevant to that sample?

A  Details of all sample sets used throughout the assessment should be identified in the “Description of Scope of Work and Approach Taken” section. Any samples reviewed for a particular testing procedure should also be identified (number and type of items in the sample) in the findings for that testing procedure.

Q 9  How will the “appropriateness” of a sample be measured?

A  The details required in the “Description of Scope of Work and Approach Taken” section of the ROC provide the assessor’s justification of why the samples chosen are appropriate.

Q 10 If a sample used to validate a requirement includes devices that are not applicable that requirement, should we include those devices in the response?

A  The assessor should only include information relevant to the finding for each requirement.

Q 11 If sampling was used to validate a testing procedure but was not defined in the testing procedure, and thus the “Identify sample” column isn’t checked, does the sample need to be identified?

A  Yes, if sampling was used to determine a finding, the assessor should include details of the sample even if there is no “Identify sample” check mark for that testing procedure.
**Description of Scope of Work and Approach Taken**

Q 12 In the “Description of Scope of Work and Approach Taken” section of the ROC, why are assessors asked to describe the network and segmentation in such detail?

A It is expected that the assessor understands the environment and any segmentation controls that are implemented so they can properly validate that the scope of the assessment is correct. The level of detail provided in the ROC should be sufficient for the reader to understand the scope and how it was validated.

**Details about Reviewed Environment**

Q 13 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.

**PCI DSS Testing Procedure 2.2.d**

Q 14 Testing procedure 2.2.d is greyed-out in the PCI DSS but the Reporting Instructions include reporting details for this testing requirement. How should assessors report this in the ROC?

A The “In Place” and “Comment” fields were greyed out in error in PCI DSS 2.0. Assessors should continue to verify that system configuration standards include the secure configuration principles defined in Requirements 2.2.1 through 2.2.4.

**PCI DSS Testing Procedure 3.3**

Q 15 For PCI DSS Requirement 3.3, are we required to list all personnel who have access to full PANs?

A The reporting details for PCI DSS Requirement 3.3 include the following:

- Identifying all instances where PANs are displayed (for example, POS terminals, transaction reports, database views, etc);
- Identifying the document that defines the organization’s policy for masking PAN and that identifies those with a business need to see full PAN (for example, by role or job function); and
- Observing each type of instance to confirm that only those defined as having a legitimate business need can actually view the full PAN (for example, through observation of access control lists, role assignments, etc).

It is not a requirement that the ROC include a list of personnel with such access.
PCI DSS Testing Procedure 6.2.a

Q 16 Why is the “Observe process, action, state” column marked in a different color for Testing Procedure 6.2.a?

A The following item in the “Reporting Details” column refers to the risk-ranking portion of Testing Procedure 6.2.a, which is not a requirement until June 30, 2012. Assessors are therefore not required to report on this item until then:

- If risk ranking is assigned to new vulnerabilities, briefly describe the observed process for assigning a risk ranking, including how critical, highest risk vulnerabilities are ranked as “High.”

See the section “Compensating Controls, Not Applicable, and Future-Dated Requirements” on page 9 for additional guidance on how to handle future-dated requirements.

PCI DSS Testing Procedures 10.3.1 - 10.3.6

Q 17 Are 14 individual statements needed for each of PCI DSS Requirements 10.3.1 – 10.3.6?

A Separate statements are not required for every reporting detail. For example, if the same personnel are interviewed for all logged events, this can be communicated in one statement. However, it must be clear to the reader that all aspects of the requirement and testing procedure have been assessed and validated.