Payment Card Industry
Payment Application Data Security Standard (PA-DSS)

FAQs for use with ROV Reporting Instructions
for PA-DSS version 2.0

March 2012

ROV Reporting Instructions for PA-DSS v2.0
Frequently Asked Questions (FAQs)

Purpose of document

This document addresses questions around the use of the ROV Reporting Instructions for PA- 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 "ROV 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 application 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 application from one assessment to the next?

A. Assessors are expected to perform a fresh assessment each time, as the results from previous assessments are not necessarily relevant for a current assessment. Where a finding happens to be the same from one assessment to the next, the details provided in the ROV may be similar but they should not be duplicates. Each requirement should be reviewed against the current application version such that the assessment findings are current and independent of previous 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.

Q6 How should I address the critical test procedures identified on page 11?

A. Critical test procedures address control areas that have historically been targeted by attackers attempting to compromise payment applications. These are included in the ROV Reporting Instructions for informational purposes only; assessors must ensure that all testing procedures are thoroughly assessed and findings properly documented in the ROV.

Q7 I'm concerned that documenting responses according the Reporting Instructions will significantly increase the length of the report

A. The format of responses in a ROV is not expected to mirror the format of the Reporting Instruction's Reporting Details column. The information provided in the Reporting Details column is bulleted and indexed for ease of readability; it is not intended that PA-QSAs follow this format when writing a ROV. However, PA-QSAs should ensure that they include all the required information in each response. Additionally, while the ROV must follow the template provided in the "Instructions and Content for Report on Validation" section of the PA-DSS Requirements and Testing Procedures, it is permissible and encouraged that the width of columns be adjusted to enhance the readability of the report.

Q8 When are assessors expected to start using the Reporting Instructions, is there an effective date? How does this affect assessments which are already in progress?

A. The Reporting Instructions are effective upon publication. However the PCI SSC recognizes there will be a transition period for assessors to adapt their report templates, and will take this into consideration for assessments already in progress. (Note: The transition period is not expected to exceed two months from the publication date of the Reporting Instructions).

Q9 What do these Reporting Instructions mean to me as an assessor?

A. These Reporting Instructions are intended to provide clear direction for all PA-QSAs on how to document their findings in an ROV. The PCI SSC has taken great care to ensure that the Reporting Instructions are aligned with the intent of each PA- DSS requirement. The Reporting Instructions do not replace PA-DSS testing procedures nor do they introduce new requirements. Assessors should make use of the Reporting Instructions when preparing their ROV and ensure their quality assurance processes are amended as appropriate.

Q10 Why is there an observation checkmark for some Implementation Guide testing procedures?

A. Verifying Implementation Guide content often includes verifying that the information provided to customers is consistent with how the application is observed to function. Additionally, some testing procedures require assessors to validate that the information provided in the Implementation Guide is accurate and effective, such that performing the instructions results in the requirement being met.

ROV Section and PA-DSS Testing Procedure Questions

PA-DSS Testing Procedure 1.1.c

Q 11 Testing Procedure 1.1.c is greyed-out in the PA-DSS but the Reporting Instructions include reporting details for this testing procedure. How should assessors report this in the ROV?

A. Testing Procedure 1.1.c defines the methodology to be followed for subsequent testing procedures (1.1.1 through 1.1.3). Assessors are expected to complete numerous test transactions that simulate all functions of the payment application as part of their assessment of each of the subsequent requirements. Because Testing Procedure 1.1.c does not by itself result in an assessment finding, the "In Place" column is greyed out in the PA-DSS Requirements and Security Assessment Procedures. However, assessors are expected to ensure that Testing Procedure 1.1.c is followed when assessing the subsequent testing procedures. The reporting instruction is included for Testing Procedure 1.1.c to allow assessors to document the details here, rather than potentially having to repeat this information for each of the Testing Procedures 1.1.1, 1.1.2 and 1.1.3.

PA-DSS Testing Procedure 1.1.4

Q 12 Testing Procedure 1.1.4.a requests the assessor to describe how the process provided in the PA-DSS Implementation Guide for removing historical data was observed to be effective – how is this different from Testing Procedure 1.1.4.c ?

A. These testing procedures work together to ensure that any sensitive authentication data stored by previous versions of the application is securely deleted. Testing Procedure 1.1.4.a requires the assessor to verify that the PA-DSS Implementation Guide gives appropriate instructions for the removal of any such data and that the instructions are accurate and work effectively. Testing Procedure 1.1.4.c, through the use of forensic tools and/or methods, verifies that the process results in the secure removal of data.

PA-DSS Testing Procedures 4.3.1 - 4.3.6

Q 13 Are 7 individual statements needed for each of PA-DSS Requirements 4.3.1 – 4.3.6?

A. Separate statements are not required for every reporting detail. For example, if the required audit trail entry was observed 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.

PA-DSS Testing Procedure 5.3.b

Q 14 Testing Procedure 5.3.b is greyed-out in the PA-DSS but the Reporting Instructions include reporting details for this testing procedure. How should assessors report this in the ROV?

A. Testing Procedure 5.3.b defines the methodology to be followed for subsequent testing procedures (5.3.1 through 5.3.4). Assessors are expected to identify the sample of recent payment application changes and then conduct Testing Procedures 5.3.1 through 5.3.4 on each change within the sample. Because Testing Procedure 5.3.b does not by itself result in an assessment finding, the "In Place" column is greyed out in the PA-DSS Requirements and Security Assessment Procedures. However, assessors are expected to ensure that Testing Procedure 5.3.b is followed when assessing the subsequent testing procedures. A reporting instruction has been included for Testing Procedure 5.3.b for the assessor to document their sampling response, rather than having to repeat this information for each of the Testing Procedures 5.3.1 – 5.3.4.

PA-DSS Testing Procedure 5.3.3.b

Q 15 Testing Procedure 5.3.3.b requires that all changes are tested for compliance with PA-DSS Requirement 5.2 – does the response have to list all of the vulnerabilities included in Testing Procedures 5.2.1 through 5.2.9?

A. Separate statements are not required for every reporting detail. For example, if the documented functionality testing verifies that the change was tested for all vulnerabilities defined in Requirements 5.2.1 through 5.2.9, 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.

PA-DSS Testing Procedure 5.4.a

Q 16 Should every running operating system service and daemon be listed in the ROV?

*A This testing procedure requires the assessor to identify which services, protocols, daemons, components and dependent software and hardware are enabled or required by the application, in order to verify that each of these is necessary and secure. The ROV should contain a description of **how** the assessor verified that all such items were identified and how they were confirmed to be necessary and secure. It is not expected that lists of the services, protocols, daemons, components and dependent software and hardware are included in the ROV response; however, the assessor would be expected to retain such detail in their work papers.*

PA-DSS Testing Procedure 6.1

Q 17 Testing Procedure 6.1 is greyed-out in the PA-DSS but the Reporting Instructions include reporting details for this testing procedure. How should assessors report this in the ROV?

A. Testing Procedure 6.1 identifies whether the application uses wireless technology and whether wireless applications are bundled with the payment application. This verification provides the foundation for the subsequent wireless testing procedures (6.1.a through 6.1.e).
Because Testing Procedure 6.1 does not by itself result in an assessment finding, the "In Place" column is greyed out in the PA-DSS Requirements and Security Assessment Procedures. However, assessors are expected to perform this verification as part of their assessment of the subsequent testing procedures. A reporting instruction has been included for Testing Procedure 6.1 for the assessor to record this verification, as it provides relevant context for the subsequent testing procedures.

PA-DSS Testing Procedure 6.2.b

Q 18 Can Testing Procedure 6.2.b ever be marked as "Not Applicable"?

A. The intention of this testing procedure is to ensure that, if the application could potentially be implemented into a wireless environment, the merchant is given instruction on how to do this in a PCI DSS compliant manner. If the application cannot be implemented into a wireless environment, the assessor must describe within the ROV how this restriction was verified as being enforced by the application.

PA-DSS Testing Procedures 10.3.2.a – 10.3.2.b

Q 19 PA-DSS Requirement 10.3.2 contains a list of examples of remote access security features – do all of these examples have to be included in the ROV?

A. The remote access security features included in Requirement 10.3.2 are provided as examples of the types of controls that may be implemented. Testing Procedure 10.3.2.a requires the PA-QSA to identify the actual remote access security features which have been implemented and confirm how those features were observed to be used. Testing Procedure 10.3.2.b requires the PA-QSA to describe how the PA-DSS Implementation Guide provides instructions for the implementation and use of remote access security features appropriate to the application.

PA-DSS Testing Procedure 11.1.a

Q 20 If the application allows and/or facilitates sending of PANs by end-user messaging technologies, how should this be included in the ROV?

A. If the application allows and/or facilitates sending of PANs by end-user messaging, the vendor must either provide strong cryptography and security protocols with the application or specify the use thereof. If the vendor specifies use of strong cryptography and security protocols, the PA-QSA must identify the documentation that contains the instructions specifying such use.

PA-DSS Testing Procedure 13.1

Q 21 Requirement 13.1 requires observation of development of the PA-DSS Implementation Guide but this document should be developed before the assessment takes place – how can this be resolved?

A. This testing procedure verifies that the vendor has a process for developing, maintaining and disseminating the PA-DSS Implementation Guide. The PA-QSA must briefly describe this process in the ROV and describe how the process was observed to be implemented.