Payment Card Industry (PCI)

Payment Application Data Security Standard (PA-DSS)

Frequently Asked Questions for use with ROV Reporting Template for PA-DSS v3.0

June 2014

ROV Reporting Template for PA-DSS v3.0: Frequently Asked Questions (FAQs)

Purpose of document

This document addresses questions around the use of the ROV Reporting Template for PA-DSS v3.0 *(PCI Reporting Template for Report on Validation, for use with PA-DSS v3.0)*.

General Questions

Q 1 What happened to the critical test procedures for PA-DSS from the *PA-DSS Program Guide v2.0* and the Reporting Instructions for PA-DSS 2.0?

A *Critical test procedures are not specifically identified in the* PA-DSS Program Guide *for 3.0 or in the ROV Reporting Template for PA-DSS v3.0. Critical test procedures were originally designated to bring attention to those control areas that have historically been targeted by attackers attempting to compromise payment applications. However, removal of the "critical test procedure" designation was indicated to eliminate confusion and reinforce messaging that assessors must ensure that all testing procedures are thoroughly assessed and that all findings must be properly documented in the ROV.*

Q 2 Which Report on Validation (ROV) should I submit for a payment application validated to PA-DSS v3.0?

A *Payment applications validated to PA-DSS v3.0 must use the ROV Reporting Template for v3.0.*

Note that until December 31, 2014, ROVs for v2.0 payment applications may be submitted using PA-DSS Program Guide v2.1*; but as of January 1, 2015 all new submissions must adhere to and be submitted in accordance with* PA-DSS Program Guide v3.0. *Be sure to fully understand the differences between the two Program Guides when considering which forms to submit during 2014.*

Q 3 How can I transition my PA-DSS v2.0 application to PA-DSS v3.0?

A *PA-DSS v2.0 payment applications will need to undergo a full PA-DSS v3.0 assessment by a PA-QSA in order for it to be considered for PA-DSS v3.0 validation.*

Q 4 I see that some of the Documentation Reviewed instructions in ROV Reporting Template for PA-DSS v3.0 are similar to those in the ROC Reporting Template for PCI DSS v3.0, but all of the ones referencing the *PA-DSS Implementation Guide* contain different instructions to "identify the page number(s)/sections" instead. Why is the Implementation Guide treated differently?

A The PA-DSS Implementation Guide *is an important part of the payment application being validated, and this adjustment to instructions for reporting on that document reflects the larger goal to support stronger* PA-DSS Implementation Guides *under PA-DSS v3.0.*

The specific document(s) that comprise of the Implementation Guide is defined by the PA-QSA in Section 2.7, "Documentation Reviewed," of the Reporting Template. An "in place" response for the testing procedures relevant to review of the PA-DSS Implementation Guide *already states that the Implementation Guide identified at 2.7 includes the details required in the testing procedure. By asking the PA-QSA to "identify the page number(s)/sections" in these responses, there is increased assurance provided that the content was identified as present.*

Q 5 Is use of the ROV Reporting Template for PA-DSS v3.0 mandatory?

A *The ROV Reporting Template for PA-DSS v3.0 is mandatory for use by PA-QSAs assessing against PA-DSS v3.0. An assessment against v3.0 of the PA-DSS by a PA-QSA must be completed using this Reporting Template, with all grey boxes and response sections completed (even if to note it is not applicable). Assessments against PA-DSS 2.0 and reporting for those have not changed, and a ROV Reporting Template for PA-DSS 2.0 is not planned for release by PCI SSC.*

Q 6 I'm confused about when to use which document versions and how to pair them up. Please explain it as simply as possible.

A *In 2014, you may assess against either 2.0 or 3.0. If you assess against 2.0, you need to use the 2.0 Reporting Instructions, Attestations for 2.0, and the other supporting 2.0 documents, such as Program Guide 2.1. You may only assess against 2.0 through the end of 2014. If you assess against 3.0, you need to use the Reporting Template for 3.0, the version 3.0 attestations and the other supporting 3.0 documents, such as Program Guide 3.0. There is NO mixing and matching of these publications allowed.*

Q 7 Where can I find the unlocked Microsoft Word version of the ROV Reporting Template for PA-DSS v3.0?

A *The most up-to-date unlocked Microsoft Word version of the ROV Reporting Template for PA-DSS v3.0 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 ROV Reporting Template for PA-DSS v3.0 during the PA-DSS v3.0 lifecycle.*

Contact your Program Manager directly if you cannot access the Assessor Portal. A PDF version of the ROV Reporting Template for PA-DSS v3.0 is available on the PCI SSC website for non-assessor inquiries.

Q 8 Can a PA-QSA company make personalization-type changes to the ROV Reporting Template for PA-DSS v3.0 and, if so, what are the limitations?

A *PCI SSC recognizes the need for personalization changes by the PA-QSA to the ROV Reporting Template for PA-DSS v3.0, such as the addition of company logos and addition of legal verbiage. Changes should be minimal, and the format of the ROV Reporting Template for PA-DSS v3.0 should remain unchanged. Generally, changes to the format should be limited to the addition of rows as needed. Nothing should be removed, including sections or requirements determined to be not applicable. Those sections and/or requirements shall remain in the completed ROV Reporting Template with the "not applicable" result documented instead.*

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

Q 9 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 10 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 PA-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 11 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 or ROV be compiled in English; however, the QSA/PA-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 12 Into what other languages will the ROV Reporting Template for PA-DSS v3.0 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 ROV Reporting Template for PA-DSS v3.0 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 PA-QSA translates this document, PCI SSC requires the following:*

1. *PA-QSA must provide both PCI SSC's English version and PA-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 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 <<PA-QSA Company>>, and PCI SSC has not had any involvement in and does not endorse the Translation. <PA-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. <<PA-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 13 What happened to the Reporting Methodology instructions and checkmarks that were in the Reporting Instructions for PA-DSS v2.0, but appear to be missing from the ROV Reporting Template for PA-DSS v3.0?

A *PCI SSC removed the Reporting Methodology instructions and checkmark columns after determining they were no longer necessary for ROV Reporting Template for PA-DSS v3.0 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 ROV Reporting Template for PA-DSS v3.0, in support of the enhanced Testing Requirements in PA-DSS v3.0, 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 14 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 ROV Template" section of the ROV Reporting Template for PA-DSS v3.0, 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 15 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 ROV Reporting Template for PA-DSS v3.0, the Reporting Instruction is present directly next to the PA-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.*

ROV Section and PA-DSS Testing Procedure Questions

PA-DSS General Reporting

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 be included in the ROV response; however, the assessor would be expected to retain such detail in their work papers.*

PA-DSS Testing Procedure 13.1

Q 17 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.*

Attestation of Validation

Q 18 My company wants to have one lead PA-QSA who signs all of the AOVs our group delivers. Is that acceptable or does the signature need to be the person who led the actual assessment?

A *The PA-QSA signature on the Attestation of Validation (AOV) should be the name and signature of the PA-QSA who led the assessment and who is asserting compliance. This should be more clear in the AOV for 3.0, as the use of the terms "Lead PA-QSA" and "Primary PA-QSA" in the AOV for 2.0 were potentially confusing. The intent, however, does remain the same.*

PA-DSS Program Guide Questions

PA-DSS Program Guide Updates

Q 19 What are the biggest changes to *PA-DSS Program Guide v2.1,* in comparison to *PA-DSS Program Guide v2.0?*

A *The* PA-DSS Program Guide v2.1 *contains minor process and terminology updates noted since PA-DSS Program Guide v2.0. We recommend that vendors and PA-QSAs fully review the Program Guide. Some of the notable changes to PA-DSS Program Guide v2.1 include:*

- *Added "Qualified Integrators and Resellers" section to explain how the new QIR Program aligns with the PA-DSS Program*
- *Updated process for submitting a ROV to allow PCI SSC to invoice the vendor upon receipt of a ROV and receive payment prior to reviewing the ROV*
- *Renamed "Quality Assurance Program" section to "Assessor Quality Management Program" and updated processes accordingly*
- *Clarified vendor requirements in Appendix A for Payment Application description*

Q 20 What are the biggest changes to *PA-DSS Program Guide v3.0,* in comparison to *PA-DSS Program Guide v2.0?*

A PA-DSS Program Guide v3.0 *contains a number of process improvements and features that are intended to provide flexibility for vendors and PA-QSAs. We recommend that vendors and PA-QSAs fully review the Program Guide. Some of the notable changes to* PA-DSS Program Guide v3.0 *include:*

- *Updated criteria and process for delta assessments*
- *Updated section on payment application change types*
- *"Change Documentation" section added to clarify process requirements*
- *Added section and Appendix B for wildcard versioning*
- *Former Appendix B changed to Appendix C (Identification of Certified Payment Application Builds)*
- *Changed "Quality Assurance Program" section to "Assessor Quality Management Program" and updated processes accordingly*
- *Clarified PA-QSA Company laboratory requirements*
- *Added Appendix D: PA-QSA Change Impact [document template]*

Q 21 What are the effective dates of the *PA-DSS Program Guide v3.0?*

A PA-DSS Program Guide v3.0 *is effective and available for use as of February 2014. PA-DSS Program Guide v3.0 becomes mandatory for all new payment applications on January 1, 2015.*

Q 22 Is there a transition period from *PA-DSS Program Guide v2.1* to *v3.0?*

A *Yes, payment applications may be validated against either PA-DSS v2.0 (using* PA-DSS Program Guide v2.1*), or PA-DSS v3.0 (using* PA-DSS Program Guide v3.0*) through December 31, 2014. After December 31, 2014:*

- *New payment applications must be validated against PA-DSS v3.0 (using* PA-DSS Program Guide v3.0*)*
- *Payment applications validated against PA-DSS v2.0 will be listed as Acceptable for New Deployments until October 28, 2016, as long as they meet annual revalidation requirements.*

Changes to Listed Payment Applications

Q 23 Can a No Impact or Low Impact Change (per *PA-DSS Program Guide v2.0*) be submitted to transition a PA-DSS v2.0 application to PA-DSS v3.0?

A *No, PA-DSS v2.0 payment applications will need to undergo a full PA-DSS v3.0 assessment by a PA-QSA in order for it to be considered for PA-DSS v3.0 validation.*

Q 24 Do No Impact changes require change submission to PCI SSC under PA-DSS Program Guide v3.0?

A *If the vendor has chosen to use a wildcard versioning methodology for managing No Impact changes (in accordance with* PA-DSS Program Guide v3.0 *or higher), Low Impact changes falling within the scope of wildcard usage are not required to be advised to PCI SSC, nor will the changes result in any update to the application listing on the PCI SSC website.*

If the vendor has not chosen to use a wildcard versioning methodology for managing No Impact changes, No Impact changes will require validation and submittal to PCI SSC.

Q 25 Can I submit minor changes for a v2.0 payment application after December 31, 2014?

A *Yes, "minor changes" (as defined in* PA-DSS Program Guide v2.1*) may be submitted for PA-DSS v2.0 payment applications until October 28, 2016.*

Q 26 Does a No Impact or Low Impact change affect an application's expiry date?

A *No Impact and Low Impact changes do not have any effect on an application's expiry date. Such changes may be submitted until the application expires; however, the application will still expire on its scheduled date.*

Q 27 Which Program Guide should I use to submit "minor updates" for 2.0 payment applications?

A *All changes to PA-DSS v2.0 payment applications must adhere to and be submitted in accordance with* PA-DSS Program Guide v2.1*. Vendors and assessors are not permitted to mix Program Guides.*

Q 28 Which Program Guide should I use to submit No Impact or Low Impact changes for v3.0 payment applications?

A *All changes to PA-DSS v3.0 payment applications must adhere to and be submitted in accordance with PA-DSS Program Guide v3.0. Vendors and assessors are not permitted to mix Program Guides.*

Revalidation of Listed Payment Applications

Q 29 Which Program Guide should I use to submit revalidations for v2.0 payment applications?

A *Revalidations for v2.0 payment applications must adhere to and be submitted in accordance with* PA-DSS Program Guide v2.1. *Revalidations for v2.0 payment applications will be accepted until their expiry date (October 28, 2016), after which time they will be listed as "Acceptable only for Pre-Existing Deployments."*

Effective January 1, 2015, all new payment application assessments must adhere to and be submitted in accordance with PA-DSS Program Guide v3.0 *in order to be considered for validation and listing as "Acceptable for New Deployments."*

Q 30 Which Program Guide should I use to submit revalidations for v3.0 payment applications?

A *Revalidations for v3.0 payment applications must be submitted using* PA-DSS Program Guide v3.0.

Q 31 Do I need to revalidate my v2.0 payment application after January 1, 2015?

A *Yes, if the vendor wishes to keep the payment application listed as "Acceptable for New Deployments." Revalidations for v2.0 payment applications must be submitted (using Program Guide v2.1) until the application expires on October 28, 2016. Payment applications are to be revalidated according to their annual revalidation date, which is based on the date the application was originally accepted. If a vendor chooses to not revalidate their v2.0 payment application, it will be moved to the "Acceptable only for Pre-Existing Deployments" list upon expiring.*

Q 32 Do I need to revalidate my v2.0 payment application after it expires on October 28, 2016?

A *No, revalidations will not be accepted for v2.0 payment applications after they expire on October 28, 2016.*

Q 33 What happens if I do not revalidate my v2.0 payment application prior to its expiry date?

A *Payment applications not revalidated prior to their expiry date (October 28, 2016, for v2.0 applications) will expire upon the date of missed revalidation. Expired applications are listed as "Acceptable only for Pre-Existing Deployments."*

Q 34 Should I revalidate my v2.0 application before it expires in October 2016?

A *Prior to a v2.0 payment application's expiry on October 28, 2016, the vendor may choose to either:*

- *Revalidate their application so they can be listed as "Acceptable for New Deployments" until October 28, 2016. After October 28, 2016, all v2.0 payment applications will be listed as "Acceptable only for Pre-Existing Deployments."*

OR

- *Not revalidate their payment application, in which case the application will expire and be listed as "Acceptable only for Pre-Existing Deployments" upon the date of missed revalidation.*

Q 35 How can I extend the expiry date of my v2.0 application beyond October 28, 2016?

A *All v2.0 payment applications expire on October 28, 2016, and will be listed as "Acceptable only for Pre-Existing Deployments" after this date. To extend a payment application's expiry date and keep it listed as "Acceptable for New Deployments," vendors must submit a new PA-DSS v3.0 for the application.*