Security Standards Council™

Payment Card Industry (PCI)

Payment Application Data Security Standard (PA-DSS)

Program Guide

Version 2.0

January 2012

Document Changes

<table>
<tr><th>Date</th><th>Version</th><th colspan="2">Description</th></tr>
<tr><td>October 1, 2008</td><td>1.2</td><td colspan="2">To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.</td></tr>
<tr><td>July 2009</td><td>1.2.1</td><td colspan="2">To align content with new PCI DSS v1.2.1 and to implement minor changes noted since original v1.2.</td></tr>
<tr><td rowspan="17">January 2012</td><td rowspan="17">2.0</td><td colspan="2">The PA-DSS Program Guide has been completely reorganized to address the needs of the different types of readers that are intended to use this document to facilitate their search for pertinent program information.
Specific changes include:</td></tr>
<tr><th>Description</th><th>Pages</th></tr>
<tr><td>Updated list of references.</td><td>3</td></tr>
<tr><td>Additional terminology added.</td><td>3-4</td></tr>
<tr><td>Roles & Responsibilities have been updated to create a more consistent message on how different organizations participate in the PA-DSS program.</td><td>5-8</td></tr>
<tr><td>All process diagrams have been updated with amended processes.</td><td>10-13</td></tr>
<tr><td>PA-DSS applicability to payment applications on hardware terminals has been updated to reflect new text of the PA-DSS v2.0.</td><td>15-16</td></tr>
<tr><td>Changes to the fee structure.</td><td>19, 25</td></tr>
<tr><td>Update to the annual revalidation process.</td><td>20</td></tr>
<tr><td>Update to the process for acceptance of minor changes, including a new allowance for changes that have low impact on the PA-DSS requirements.</td><td>20-24</td></tr>
<tr><td>New payment application types added.</td><td>38-39</td></tr>
<tr><td>Information on expiry updated to reflect new 3-year lifecycle of PA-DSS.</td><td>40</td></tr>
<tr><td>The PA-DSS Attestations of Validation have been combined into a single document that combines new assessments, annual revalidations, & minor changes. In addition, it has been segregated into its own document.</td><td>N/A</td></tr>
<tr><td>New information added in the following areas:</td><td></td></tr>
<tr><td>▪ Portal used for submission of payment application assessments;</td><td>18-19, 28-30</td></tr>
<tr><td>▪ Additional detail of the PA-DSS quality assurance program; and</td><td>30-34</td></tr>
<tr><td>▪ Notation for dependencies on other PA-DSS accepted payment applications, PTS-accepted POIs, or external environments.</td><td>39</td></tr>
</table>

Table of Contents

1 Introduction

1.1 Related Publications

The following documents are the basis for payment application assessments:

- *Payment Card Industry (PCI) Payment Application Data Security Standard – Requirements and Security Assessment Procedures ("PA-DSS")*
- *Payment Card Industry (PCI) Data Security Standard - Report on Validation Reporting Instructions for PA-DSS v2.0 ("ROV Reporting Instructions")*
- *Payment Application Data Security Standard (PA-DSS) Attestation of Validation ("AOV")*

The following additional documents are used in conjunction with the aforementioned:

- *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures ("PCI DSS")*
- *Payment Card Industry (PCI) Data Security Standard and Payment Application Data Security Standard Glossary of Terms, Abbreviations, and Acronyms (the "Glossary")*
- *Payment Card Industry (PCI) Data Security Standard QSA Qualification Requirements ("QSA Qualification Requirements")*
- *Payment Card Industry (PCI) Data Security Standard QSA Qualification Requirements – Supplement for Payment Application Qualified Security Assessors (PA-QSAs) ("PA-QSA Supplement")*
- *Payment Card Industry PA-DSS Vendor Release Agreement ("PA-DSS VRA")*

Note:

- *The* PA-DSS Requirements and Security Assessment Procedures *and the* Glossary *list and define the specific technical requirements and provide the assessment procedures and template used by PA-QSAs to validate the payment application's compliance and document the review.*
- *The ROV Reporting Instructions provide detail on how to document the findings of a PA-DSS assessment.*
- *The AOV is a declaration of a payment application's validation status with the PA-DSS.*
- *The QSA Qualification Requirements and PA-QSA Supplement together define the requirements that must be met by a PA-QSA in order to perform PA-DSS assessments.*
- *The PA-DSS VRA establishes the terms and conditions under which validation of a payment applications are accepted by PCI SSC.*

PCI DSS *provides the foundation for all the afore-mentioned.*

All of the above documents are available in electronic form on www.pcisecuritystandards.org (the "PCI SSC website").

1.2 Updates to Documents and Security Requirements

Security is a never-ending race against potential attackers. As a result, it is necessary to regularly review, update and improve the security requirements used to evaluate payment applications. As such, PCI SSC endeavors to publish formal updates to its payment application security requirements every 36 months. Additionally, PCI SSC provides interim updates to the PCI community through a variety of means, including required PA-QSA training, email bulletins, frequently asked questions and others.

PCI SSC reserves the right to change, amend or withdraw security requirements at any time. If such a change is required, PCI SSC will endeavor to work closely with PCI SSC's community of Participating Organizations and software vendors to help minimize the impact of any changes.

1.3 Terminology

Throughout this document the following terms have the meanings shown in the chart below.

Term	Meaning
Accepted, or listed	A payment application is deemed to have been "Accepted" or "listed" (and "Acceptance" is deemed to have occurred) when PCI SSC has: (i) received the corresponding Report on Validation from the PA-QSA; (ii) confirmed that the ROV is correct as to form, the PA-QSA properly determined that the payment application is eligible to be a PA-DSS Validated Payment Application, the PA-QSA adequately reported the PA-DSS compliance of the payment application in accordance with PA-DSS Program requirements, and the detail provided in the ROV meets PCI SSC's reporting requirements; (iii) received the *PA-DSS Payment Application Acceptance Fee* and all documentation required with respect to the payment application as part of the PA-DSS Program; and (iv) listed the payment application on the List of Validated Payment Applications; provided that PCI SSC may suspend, withdraw, revoke, cancel or place conditions upon (including without limitation, complying with remediation requirements) Acceptance of any payment application in accordance with applicable PA-DSS Program policies and procedures.
List of Validated Payment Applications	Refers to the Council's authoritative list of PA-DSS Validated Payment Applications appearing on the PCI SSC website.
Listing or listing	Refers to the listing and related information regarding a payment application on the List of Validated Payment Applications.
PCI SSC	Refers to the PCI Security Standards Council LLC
PABP	Refers to Visa's former Payment Application Best Practices program, upon which the Payment Application Data Security Standard ("PA-DSS") was based. Payment applications that were transitioned from the PABP program are identified on the PCI SSC's List of Validated Payment Applications and specifically notated as being validated under the PABP requirements.
Payment brands and Members	Each refers to the payment card brands that are statutory members of PCI SSC, currently the following or affiliates thereof: American Express, Discover, JCB, MasterCard Worldwide, and Visa.
Payment Applications	Refer broadly to all payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.
PA-DSS Program	Refers to PCI SSC's program and requirements for qualification of PA-QSAs and validation and Acceptance of payment applications, as further described in this document and related PCI SSC documents, policies and procedures.

Term	Meaning
PA-DSS Validated Payment Application	Refers to a Payment Application that has been assessed and validated by a PA-QSA as being compliant with the PA-DSS, and then Accepted by PCI SSC, so long as such Acceptance has not been revoked, suspended, withdrawn or terminated.
ROV	A “PA-DSS Report on Validation” provided by a PA-QSA to PCI SSC for purposes of demonstrating compliance with the PA-DSS as part of the PA-DSS Program.

1.4 About PCI SSC

PCI SSC reflects a desire among constituents of the Payment Card Industry (PCI) at all levels for a single, standardized set of security requirements, security assessment procedures, and processes for recognizing payment applications validated by a PA-QSA. The PA-DSS and related PCI SSC standards define a common security assessment framework that is recognized by all payment brands.

Stakeholders in the payments value chain benefit from these requirements in a variety of ways, including but not limited to the following:

- Customers benefit from a broader selection of secure payment applications.
- Customers are assured that they will be using products that have been validated to meet the PA-DSS requirements by a PA-QSA
- Vendors will only need to validate their payment application against the PA-DSS Program in order for their payment applications to be recognized by all participating payment brands.

For more information regarding PCI SSC, see the PCI SSC website.

1.5 PA-DSS Alignment Initiative and Overview

This Payment Card Industry PA-DSS Program Guide reflects a single set of requirements currently recognized by all payment brands regarding:

- Payment application security requirements and assessment procedures
- Processes for recognizing PA-QSA validated payment applications
- Quality assurance processes for PA-QSAs

Note:

PA-DSS ROVs are reviewed and accepted directly by PCI SSC.

Depending on the circumstances, a vendor that does not store, process, or transmit cardholder data may not be directly required to comply with the PCI DSS since only entities that do store, process, or transmit cardholder data are required to comply with the PCI DSS. However, since payment applications are used by customers to store, process, and transmit cardholder data, and customers are required to be PCI DSS compliant, payment applications should facilitate, and not prevent, the customers' PCI DSS compliance. Examples of how payment applications can prevent PCI DSS compliance include:

1. Magnetic-stripe data stored in the customer's network after authorization;
2. Applications that require customers to disable other features required by the PCI DSS, like anti-virus software or firewalls, in order to get the payment application to work properly; and

3. Vendor's use of unsecured methods to connect to the application to provide support to the customer.

Secure payment applications, *when implemented into a PCI DSS-compliant environment*, will help to minimize the potential for security breaches leading to compromises of full magnetic stripe data, card validation codes and values (CAV2, CID, CVC2, CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches.

1.6 Roles and Responsibilities

There are several stakeholders in the payment application community. Some of these stakeholders have a more direct participation in the PA-DSS assessment process – vendors, PA-QSAs and PCI SSC. Other stakeholders that are not directly involved with the payment application assessment process should be aware of the overall process to facilitate their associated business decisions.

The following defines the roles and responsibilities of the stakeholders in the payment application community.

1.1.1 Payment Brands

The payment brands are responsible for developing and enforcing their own programs related to PA-DSS compliance, including, but not limited to, the following:

- Any requirements, mandates, or dates for use of PA-DSS compliant payment applications; and
- Any fines or penalties related to use of non-compliant payment applications.

The payment brands define their own related compliance programs, mandates, dates, etc., as well as other requirements for using PA-DSS and PA-DSS Validated Payment Applications.

1.1.2 Payment Card Industry Security Standards Council (PCI SSC)

PCI SSC is the standards body that maintains the payment card industry standards, including the PCI DSS and PA-DSS. In relation to PA-DSS, PCI SSC:

- Is a centralized repository for all ROVs;
- Hosts the List of PA-DSS Validated Payment Applications on the PCI SSC website;
- Qualifies and provides required training for PA-QSAs to assess and validate payment applications for PA-DSS compliance;
- Maintains and updates the PA-DSS standard and related documentation according to a standards lifecycle management process; and
- Performs Quality Assurance (QA) reviews of PA-DSS ROVs to confirm report consistency and quality, including but not limited to the following:
    - Submissions (including ROVs, Minor Updates and Annual Revalidations) are correct as to form;
    - The PA-QSA properly determined that the candidate payment applications is eligible to be a PA-DSS Validated Payment Application (PCI SSC reserves the right to reject or de-list any payment application determined to ineligible for the PA-DSS Program);
    - The PA-QSA adequately reported the PA-DSS compliance of candidate payment applications in their associated Submissions; and

- Detail provided in the Submissions meets PCI SSC's reporting requirements.

Additionally, as part of the above QA process, PCI SSC assesses whether overall, PA-QSA Company operations appear to conform to PCI SSC's quality assurance and qualification requirements.

***Please Note**: PCI SSC does not assess or validate payment applications for PA-DSS compliance. As described further below, assessment and validation is the role of the PA-QSA. Listing of a payment application on the List of Validated Payment Applications signifies that the applicable PA-QSA has determined that the application complies with the PA-DSS, that the PA-QSA has submitted a corresponding ROV to PCI SSC, and that the ROV, as submitted to PCI SSC, has satisfied all applicable QA ROV review requirements as of the time of PCI SSC's review.*

1.1.3 Software Vendors

Software vendors ("vendors") that develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, and then sell, distribute, or license these payment applications to third parties (customers or resellers/integrators), are responsible for:

- Creating PA-DSS compliant payment applications that facilitate and do not prevent their customers' PCI DSS compliance (The application cannot require an implementation or configuration setting that violates a PCI DSS requirement.);
- Following the best practices of the PCI DSS requirements whenever the vendor stores, processes or transmits cardholder data (for example, during customer troubleshooting);
- Creating a *PA-DSS Implementation Guide*, **specific to each application**, in accordance with the requirements in the *Payment Application Data Security Standard;*
- Educating customers, resellers, and integrators on how to install and configure the payment applications in a PCI DSS-compliant manner;
- Ensuring their payment applications meet PA-DSS requirements by successfully passing a PA-DSS review as specified in *PCI PA-DSS Requirements and Security Assessment Procedures*; and
- Providing their customers (either directly or indirectly through their resellers and integrators) with a copy of the validated payment application's *PA-DSS Implementation Guide.* This includes any subsequent updates to the *PA-DSS Implementation Guide* that may result from changes to the payment application over time.

Vendors submit their payment applications and supporting documentation to the PA-QSA for review. Any agreements and costs associated with the PA-QSA's assessment are negotiated between the vendor and the PA-QSA. Vendors provide permission for their PA-QSA to submit resulting ROVs and related information to PCI SSC.

1.1.4 PA-QSAs

***Note:** Not all QSAs are PA-QSAs—there are additional qualification requirements that must be met for a QSA to become a PA-QSA.*

PA-QSAs are QSAs that are qualified by PCI SSC to perform PA-DSS reviews.

PA-QSAs are responsible for:

- Performing assessments on payment applications in accordance with the PA-DSS Security Assessment Procedures and the PA-QSA Validation Requirements;
- Providing an opinion regarding whether the payment application meets PA-DSS requirements;

- Providing adequate documentation within the ROV to demonstrate the payment application's compliance to the PA-DSS;
- Submitting the ROV to PCI SSC, along with the Attestation of Validation (Appendix C of the PA-DSS, signed by both PA-QSA and vendor);
- Submitting the payment application's *PA-DSS Implementation Guide* to PCI SSC;
- Maintaining an internal quality assurance process for their PA-QSA efforts;
- Staying up to date with Council statements and guidance, and industry trends and best practices;
- Determining whether or not payment applications are eligible for PA-DSS validation; and
- Satisfying all applicable PA-QSA validation requirements at all times, including but not limited to successful completion of annual revalidation and all required training and examinations.

It is the PA-QSA's responsibility to assess a payment application's compliance to the PA-DSS, as of the date of the assessment, and document their findings and opinions on compliance. As indicated above, PCI SSC does not approve ROVs from a technical compliance perspective, but performs quality assurance to confirm that the ROVs adequately document the demonstration of compliance.

1.1.5 Resellers and Integrators

Resellers and Integrators are those entities that sell, install, and/or service payment applications on behalf of software vendors or others. Resellers and integrators performing services relating to PA-DSS Validated Payment Applications are responsible for:

- Implementing PA-DSS Validated Payment Applications into a PCI DSS compliant environment (or instructing the merchant to do so);
- Configuring such payment applications (where configuration options are provided) according to the payment application's *PA-DSS Implementation Guide* provided by the vendor;
- Configuring such payment applications (or instructing the merchant to do so) in a PCI DSS compliant manner;
- Servicing such payment applications (for example, troubleshooting, delivering remote updates, and providing remote support) according to the *PA-DSS Implementation Guide* and PCI DSS; and
- Ensuring that customers are provided (either directly from the software vendor or from the reseller or integrator) with a current copy of the validated payment application's *PA-DSS Implementation Guide*.

Resellers and integrators do not submit payment applications for assessment. Products can only be submitted by the software vendor.

1.6.1 Customers

Customers are merchants, service providers, or others who buy or receive a third-party payment application to store, process, or transmit cardholder data as part of authorizing or settling of payment transactions. Customers who want to use PA-DSS applications to facilitate their PCI DSS compliance are responsible for:

Note:

A PA-DSS Validated Payment Application alone is not a guarantee of PCI DSS compliance.

- Ensuring that the payment application's version information matches what is indicated on the PCI SSC website;
- Implementing such applications into a PCI DSS compliant environment;
- Configuring each such application (where configuration options are provided) according to the payment application's *PA-DSS Implementation Guide* provided by the vendor;
- Configuring each such application in a PCI DSS-compliant manner; and
- Maintaining the PCI DSS-compliant status of both the environment and the payment application configuration.

Customers and others can find the List of Validated Payment Applications on the PCI SSC website along with other reference materials. PCI SSC's List of Validated Payment Applications is **the Council's authoritative source** for payment applications that may be used to facilitate a Customer's PCI DSS compliance requirements.

2 Overview of PA-DSS Validation Processes

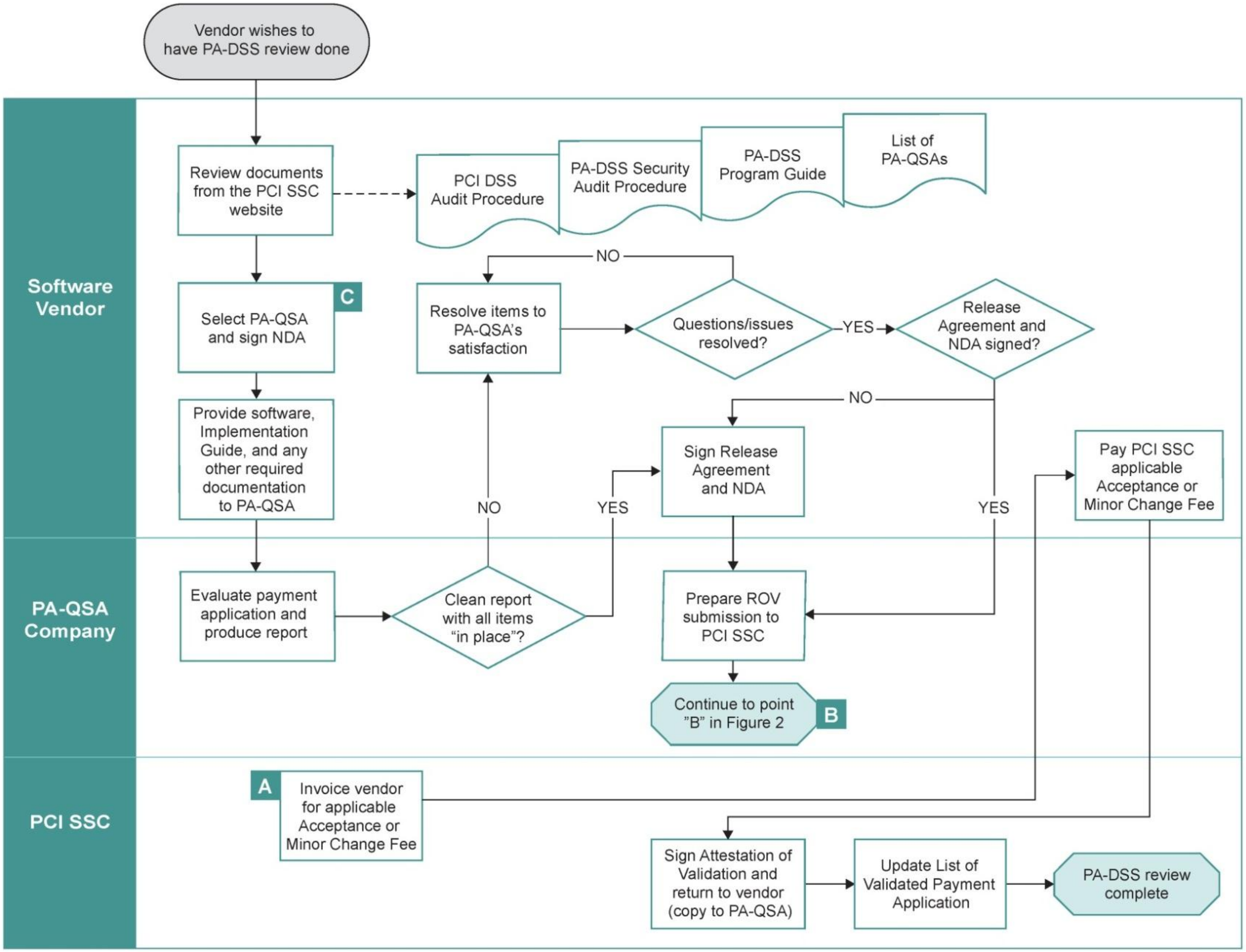
The PA-DSS review process is initiated by the vendor. The PCI SSC website has all of the associated documents the vendor will need to navigate the PA-DSS review process. The following is a high-level overview of the process:

1. The vendor selects a PA-QSA from the Council's list of recognized PA-QSAs and negotiates the cost and any associated PA-QSA confidentiality and non-disclosure agreement with the PA-QSA;
2. The vendor then provides to the PA-QSA the payment application software, corresponding PA-DSS Implementation Guide, and all associated manuals and other required documentation, including but not limited to the vendor's signed Vendor Release Agreement;
3. The PA-QSA then assesses the payment application's security functions and features to determine whether the application complies with PA-DSS security requirements;
4. If the PA-QSA determines that the payment application is in compliance with the PA-DSS, the PA-QSA submits a corresponding ROV to PCI SSC, opining to compliance and setting forth the results, opinions and conclusions of the PA-QSA on all test procedures along with the vendor's signed PA-DSS VRA;
5. PCI SSC then reviews the ROV to confirm that it meets the PA-DSS Program requirements, and if confirmed, PCI SSC will notify the PA-QSA and vendor that the payment application has successfully completed the process and issue an invoice to the vendor for the applicable *PA-DSS Payment Application Acceptance Fee*; and
6. Once the payment application is Accepted, the Council will sign a corresponding Attestation of Validation and add the payment application to the List of Validated Payment Applications on the PCI SSC website.

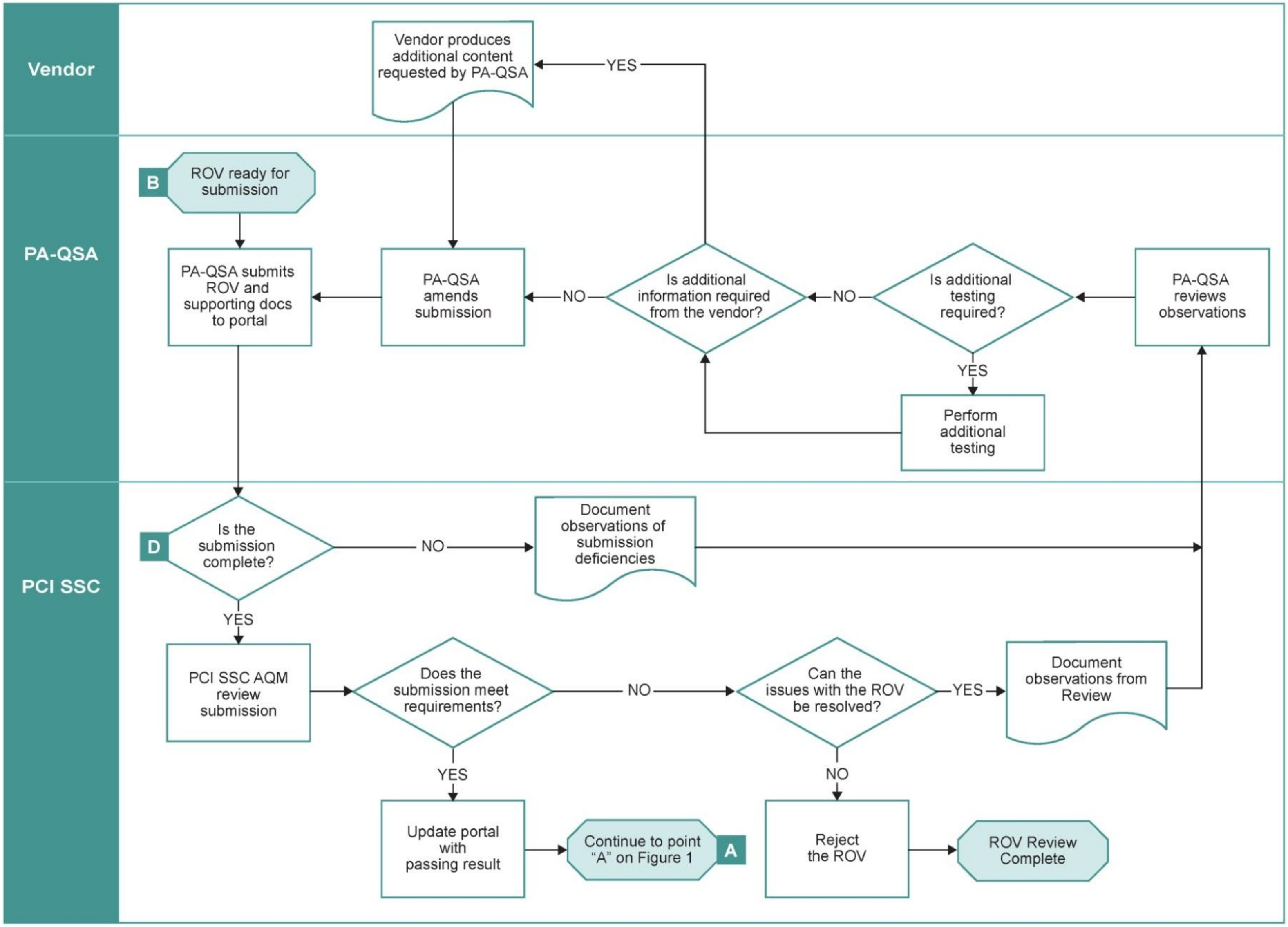
The illustrations and descriptions on the following pages explain in detail the following components of the PA-DSS program:

Process	Illustration	Page	Page Number for Related Section
PA-DSS Report on Validation Acceptance Process	Figure 1	9	16 – 19 & 27
PA-DSS Report on Validation Review Process	Figure 2	10	17 & 27 - 30
PA-DSS Annual Revalidation and Renewing Expired Applications	Figure 3	11	21 & 24
PA-DSS Minor Updates to Listed Applications	Figure 4	12	21 - 24 & 28

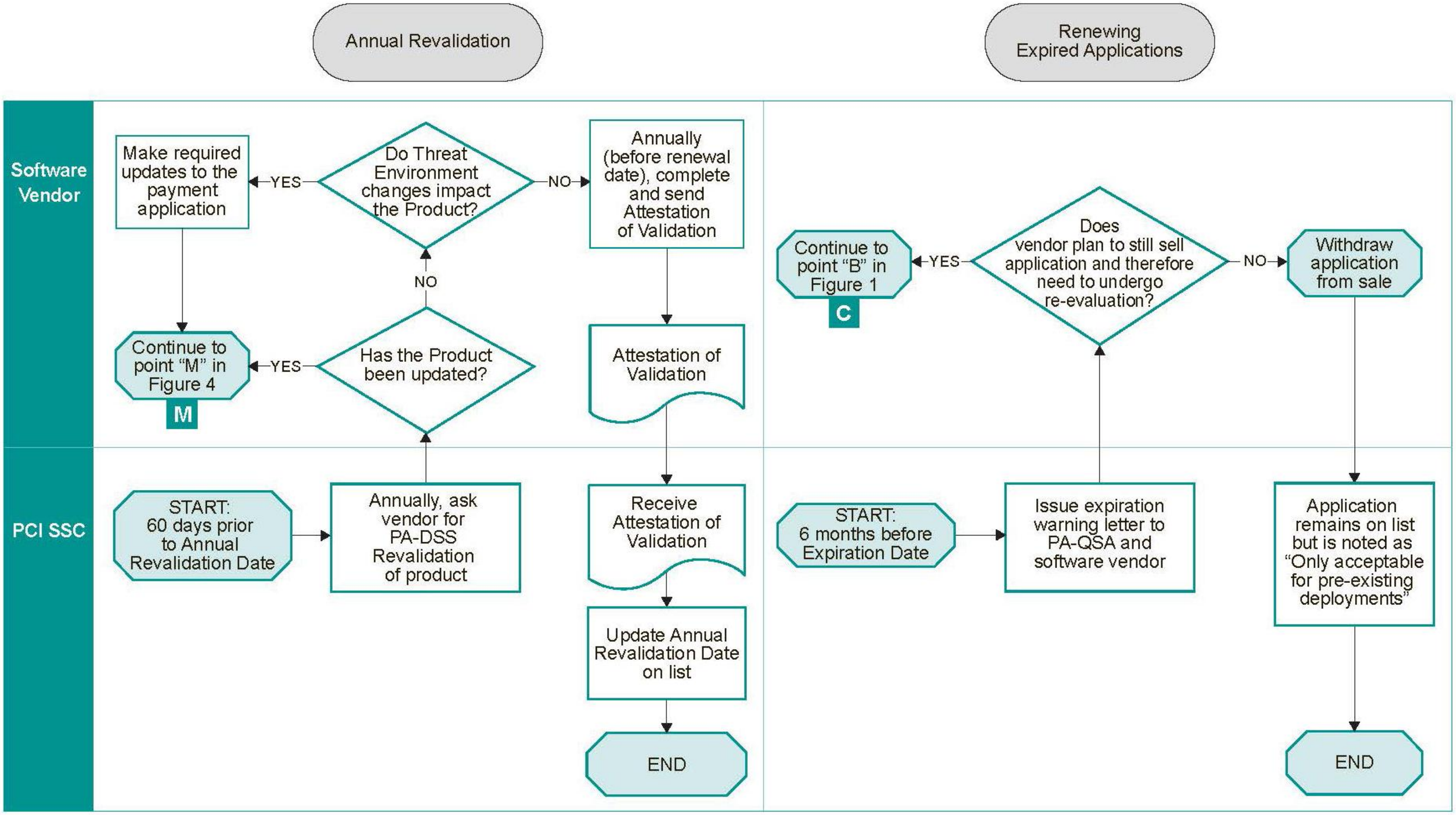
2.1 Figure 1: PA-DSS Report on Validation Acceptance Process


Vendor wishes to have PA-DSS review done
Software Vendor
PA-QSA Company
PCI SSC
Review documents from the PCI SSC website
PCI DSS Audit Procedure
PA-DSS Security Audit Procedure
PA-DSS Program Guide
List of PA-QSAs
Select PA-QSA and sign NDA
C
Resolve items to PA-QSA's satisfaction
NO
Questions/issues resolved?
YES
Release Agreement and NDA signed?
NO
Provide software, Implementation Guide, and any other required documentation to PA-QSA
NO
YES
Sign Release Agreement and NDA
YES
Pay PCI SSC applicable Acceptance or Minor Change Fee
Evaluate payment application and produce report
Clean report with all items "in place"?
Prepare ROV submission to PCI SSC
Continue to point "B" in Figure 2
B
A
Invoice vendor for applicable Acceptance or Minor Change Fee
Sign Attestation of Validation and return to vendor (copy to PA-QSA)
Update List of Validated Payment Application
PA-DSS review complete

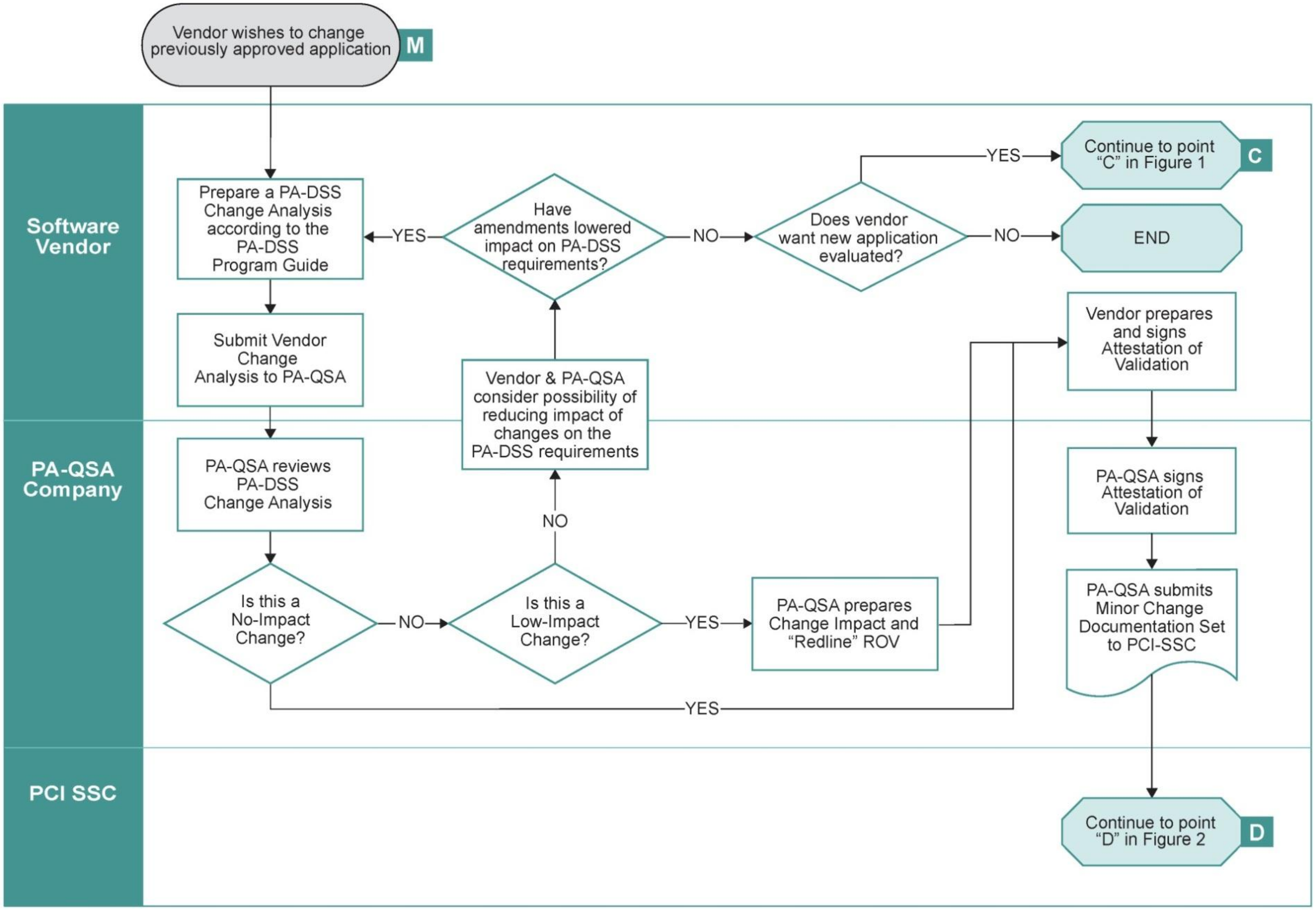
2.2 Figure 2: PA-DSS Report on Validation Review Process


Vendor
PA-QSA
PCI SSC
Vendor produces additional content requested by PA-QSA
YES
B
ROV ready for submission
PA-QSA submits ROV and supporting docs to portal
PA-QSA amends submission
NO
Is additional information required from the vendor?
NO
Is additional testing required?
PA-QSA reviews observations
YES
Perform additional testing
D
Is the submission complete?
NO
Document observations of submission deficiencies
YES
PCI SSC AQM review submission
Does the submission meet requirements?
NO
Can the issues with the ROV be resolved?
YES
Document observations from Review
YES
NO
Update portal with passing result
Continue to point “A” on Figure 1
A
Reject the ROV
ROV Review Complete

2.3 Figure 3: PA-DSS Annual Revalidation and Renewing Expired Applications


Annual Revalidation
Renewing Expired Applications
Software Vendor
PCI SSC
Make required updates to the payment application
YES
Do Threat Environment changes impact the Product?
NO
Annually (before renewal date), complete and send Attestation of Validation
NO
Continue to point "M" in Figure 4
M
YES
Has the Product been updated?
Attestation of Validation
START: 60 days prior to Annual Revalidation Date
Annually, ask vendor for PA-DSS Revalidation of product
Receive Attestation of Validation
Update Annual Revalidation Date on list
END
Continue to point "B" in Figure 1
C
YES
Does vendor plan to still sell application and therefore need to undergo re-evaluation?
NO
Withdraw application from sale
START: 6 months before Expiration Date
Issue expiration warning letter to PA-QSA and software vendor
Application remains on list but is noted as "Only acceptable for pre-existing deployments"
END

2.4 Figure 4: PA-DSS Minor Updates to Listed Applications


Vendor wishes to change previously approved application
M
Software Vendor
PA-QSA Company
PCI SSC
Prepare a PA-DSS Change Analysis according to the PA-DSS Program Guide
YES
Have amendments lowered impact on PA-DSS requirements?
NO
Does vendor want new application evaluated?
YES
Continue to point "C" in Figure 1
C
NO
END
Submit Vendor Change Analysis to PA-QSA
Vendor & PA-QSA consider possibility of reducing impact of changes on the PA-DSS requirements
Vendor prepares and signs Attestation of Validation
PA-QSA reviews PA-DSS Change Analysis
NO
PA-QSA signs Attestation of Validation
Is this a No-Impact Change?
NO
Is this a Low-Impact Change?
YES
PA-QSA prepares Change Impact and "Redline" ROV
PA-QSA submits Minor Change Documentation Set to PCI-SSC
YES
Continue to point "D" in Figure 2
D

3 Vendor Considerations – Preparation for the Review

3.1 To Which Applications does PA-DSS Apply?

For purposes of PA-DSS, a payment application is defined as one that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment applications is sold, distributed, or licensed to third parties.

The following guide can be used to determine whether PA-DSS applies to a given payment application:

- PA-DSS does apply to payment applications that are typically sold and installed "off the shelf" without much customization by software vendors.
- PA-DSS does apply to payment applications provided in modules, which typically includes a "baseline" module and other modules specific to customer types or functions, or customized per customer request. PA-DSS may only apply to the baseline module if that module is the only one performing payment functions (once confirmed by a PA-QSA). If other modules also perform payment functions, PA-DSS applies to those modules as well. Note that it is considered a "best practice" for software vendors to isolate payment functions into a single or small number of baseline modules, reserving other modules for non-payment functions. This best practice (though not a requirement) can limit the number of modules subject to PA-DSS.
- PA-DSS does not apply to payment applications offered by application or service providers only as a service (unless such applications are also sold, licensed, or distributed to third parties) because:

  1) The application is a service offered to customers (typically merchants) and the customers do not have the ability to manage, install, or control the application or its environment;
  2) The application is covered by the application or service provider's own PCI DSS review (this coverage should be confirmed by the customer); and/or
  3) The application is not sold, distributed, or licensed to third parties.

  Examples of these "software as a service" payment applications include:

  1) Those offered by Application Service Providers (ASP) who host a payment application on their site for their customers' use. Note that PA-DSS would apply, however, if the ASP's payment application were also sold to, and implemented on, a third-party site, and the application was not covered by the ASP's PCI DSS review.
  2) Virtual terminal applications that reside on a service providers' site and are used by merchants to enter their payment transactions. Note that PA-DSS would apply if the virtual terminal application has a portion that is distributed to, and implemented on, the merchant's site, and was not covered by the virtual terminal provider's PCI DSS review.
- PA-DSS does not apply to non-payment applications that are part of a payment application suite. Such applications (for example, a fraud-monitoring, scoring, or detection application included in a suite). These applications *can be, but are not required to be*, covered by PA-DSS if the whole suite is assessed together. However, if a payment application is part of a suite that relies on PA-DSS requirements being met by controls in other applications in the suite, a single PA-DSS assessment should be performed for the payment application and all other applications in the suite upon which it relies. These applications should not be assessed separately from other applications they rely upon since all PA-DSS requirements are not met within a single application.

- PA-DSS does NOT apply to a payment application developed for and sold to a single end-user customer for the sole use of that customer, since this application will be covered as part of the customer's normal PCI DSS compliance review. Note that such an application (which may be referred to as a "bespoke" application) is sold to only one customer (usually a large merchant or service provider), and it is designed and developed according to customer-provided specifications.
- PA-DSS does NOT apply to payment applications developed by merchants and service providers if used only in-house (not sold, distributed, or licensed to a third party), since this in-house developed payment application would be covered as part of the merchant's or service provider's normal PCI DSS compliance.

For example, for the last two bullets above, whether the in-house developed or "bespoke" payment application stores prohibited sensitive authentication data or allows complex passwords would be covered as part of the merchant's or service provider's normal PCI DSS compliance efforts and would not require a separate PA-DSS assessment.

Further guidance from the Council may be provided as new technologies or uses emerge. To provide direction in this area, the council maintains a document entitled *Applications Eligible for PA-DSS Validation*. This document can be found on the PCI SSC website. The following list, while not all-inclusive, illustrates other applications that are NOT payment applications for purposes of PA-DSS (and therefore are not eligible for independent assessment under PA-DSS):

- Operating systems onto which a payment application is installed (for example, Windows, Unix)
- Database systems that store cardholder data (for example, Oracle)
- Back-office systems that store cardholder data (for example, for reporting or customer service purposes)

Note:

PCI SSC will ONLY Accept and list payment applications that are eligible for a PA-DSS assessment, as defined by the PCI SSC.

3.2 PA-DSS Applicability to Payment Applications on Hardware Terminals

Payment applications designed to operate on hardware terminals (also known as a standalone or dedicated POS terminal) may undergo a PA-DSS review if the vendor wishes to achieve validation and if PA-DSS compliance requirements can be met. Reasons a vendor may wish to undergo a PA-DSS validation for a payment application on a hardware terminal include, but are not limited to, business needs and compliance obligations. This section provides guidance for vendors who wish to gain PA-DSS validation for resident payment applications on hardware terminals.

There are two ways for a resident payment application on a hardware terminal to achieve PA-DSS validation:

1. The resident payment application directly meets all PA-DSS requirements and is validated according to standard PA-DSS procedures.
2. The resident payment application does not meet all PA-DSS requirements, but the hardware that the application is resident on is listed on the PCI SSC's Approved PIN Transaction Security (PTS) Devices List as a current PCI PTS approved Point of Interaction (POI) device. In this scenario, it may be possible for the application to satisfy PA-DSS requirements through a combination of the PA-DSS and PTS validated controls.

The remainder of this section applies only to payment applications that that are resident on a validated PCI PTS approved POI device.

If one or more PA-DSS requirements cannot be met by the payment application directly, they may be satisfied indirectly by controls tested as part of the PCI PTS validation. For a hardware device to be considered for inclusion in a PA-DSS review, the hardware device MUST be validated as a PCI PTS approved POI device and be listed on the PCI SSC's Approved PTS Devices List. The PTS validated POI device, which provides a trusted computing environment, will become a "***required dependency***" for the payment application, and the combination of application and hardware will be listed together on the PA-DSS List of Validation Payment Applications.

When conducting the PA-DSS assessment, the PA-QSA must fully test the payment application with its dependant hardware against all PA-DSS requirements. If the PA-QSA determines that one or more PA-DSS requirements cannot be met by the resident payment application, but they are met by controls validated under PCI PTS, the PA-QSA must:

1. Clearly document which requirements are met as stated per PA-DSS (as usual);
2. Clearly document which requirement was met via PCI PTS in the "In Place" box for that requirement;
3. Include a thorough explanation as to why the payment application could not meet the PA-DSS requirement;
4. Document the procedures that were conducted to determine how that requirement was fully met through a PCI PTS validated control; and
5. List the PCI PTS validated hardware terminal as a required dependency in the Executive Summary of the ROV.

Once the PA-QSA's validation of the payment application is complete and is subsequently accepted by the PCI SSC, the PTS validated hardware device will be listed as a dependency for the payment application on the PA-DSS List of Validated Applications.

Resident payment applications on hardware terminals that are validated through a combination of PA-DSS and PCI PTS controls must meet the following criteria:

1. Be provided together to the customer (both hardware terminal and application), OR, if provided separately, the application vendor and/or the reseller/integrator must package the application for distribution such that it will only operate on the hardware terminal it has been validated to run on;
2. Enabled by default to support a customer's PCI DSS compliance;
3. Include ongoing support and updates to maintain PCI DSS compliance; and
4. If the application is separately sold, distributed or licensed to customers, the vendor must provide details of the dependant hardware required for use with the application, in accordance with its PA-DSS validation listing.

3.3 Prior to the Review

Prior to commencing a PA-DSS review with a PA-QSA, software vendors are encouraged to take the following preparatory actions:

- Review both PCI DSS and PA-DSS requirements and related documentation located at the PCI SSC website;
- Determine/assess your payment application's readiness to comply with PA-DSS:
    - Perform a "gap" analysis between how the payment application subject to PA-DSS functions compared to PA-DSS requirements;
    - Correct any gaps; and
    - If desired, the PA-QSA may perform a pre-assessment or "gap" analysis of a vendor's payment application. If the PA-QSA notes deficiencies that would prevent a clean opinion, the PA-QSA will provide to the software vendor a list of payment application features to be addressed before the formal review process begins; and
- Determine whether the payment application's *PA-DSS Implementation* Guide meets PA-DSS *Implementation Guide* requirements and correct any gaps.

3.4 Required Documentation and Materials

As a requirement for the assessment, the software vendor must provide the appropriate documentation and software to the PA-QSA.

All PCI SSC information and documents relevant to PA-DSS can be downloaded from the PCI SSC website. All completed payment application related materials such as install CDs, manuals, the *PA-DSS Implementation Guide*, the Vendor Release Agreement and all other materials related to the review and participation in the PA-DSS Program must be delivered to a PA-QSA listed on the PCI SSC website, not to PCI SSC.

Examples of documents and items to submit to the PA-QSA include, but not limited to:

1. The payment application;
2. The necessary hardware and software accessories to perform:
    - Simulated payment transactions; and
    - Operational support functions on the payment application;
3. Documentation that describes all functions used for data input and output that can be used by third-party application developers. Specifically, functions associated with capture, authorization, settlement and chargeback flows (if applicable to the application) must be described. (A manual is an example of documentation that could fulfill this requirement.);
4. Documentation that relates to installing and configuring the application, or which provides information about the application. Examples of such documentation include:
    - *PA-DSS Implementation Guide* (note that this *must* be submitted to the PA-QSA)*;*
    - Software Installation Guide or Instructions (as provided to customers);
    - Vendor's version-numbering scheme; and
    - Change control documentation that shows how changes are illustrated to customers;
5. Additional documentation—such as diagrams and flowcharts—that will aid in the payment application review (the PA-QSA may request additional material when necessary.); and

6. The vendor’s executed PA-DSS VRA.

3.5 PA-DSS Review Timeframes

The amount of time necessary for a PA-DSS review, from start to completion resulting in a fully validated application with all items noted as “in place,” can vary widely depending on factors such as:

- How close is the application to being PA-DSS compliant at the start of the review
  - Corrections to the payment application to achieve compliance will increase the length of time.
- How ready the payment application’s *PA-DSS Implementation Guide* is at the start of the review
  - Extensive rewrites of the PA-DSS Implementation *Guide* will increase the length of time.
- Whether the PA-QSA prepares and submits a high-quality PA-DSS ROV to PCI SSC
  - If PCI SSC reviews the ROV more than once, providing comments back to the PA-QSA to address each time, this will increase the length of time.

Any review timeframes provided by a PA-QSA should be considered estimates, since they may be based on the assumption that the payment application is able to successfully meet all PA-DSS requirements quickly. If problems are found during the review or acceptance processes, discussions between the PA-QSA, the software vendor, and/or PCI SSC will be required. Such discussions may significantly impact review times and cause delays and/or may even cause the review to end prematurely (if, for example, the vendor decides they do not want to make the necessary payment application changes to achieve compliance or it is determined that the application is not eligible for PA-DSS validation).

3.6 Payment Application Qualified Security Assessors

PCI SSC qualifies and provides required training for Payment Application Qualified Security Assessors (PA-QSAs) to assess and validate payment applications for PA-DSS compliance. In order to perform PA-DSS assessments, a PA-QSA must have been qualified by PCI SSC and remain in good standing as both a QSA and PA-QSA, and complete all required PA-QSA training. All recognized PA-QSAs are listed on the PCI SSC website. These are the only assessors recognized by PCI SSC as qualified to perform PA-DSS assessments.

The prices and fees charged by PA-QSAs are not set by PCI SSC. These fees are negotiated between the PA-QSA and their customer. Before deciding on a PA-QSA, it is recommended that a prospective customer should check PCI SSC's list of recognized PA-QSAs, talk to several PA-QSA firms, and follow their own vendor selection processes.

3.6.1 Non-PA-DSS assessment services that may be offered by PA-QSAs

The list below provides examples of non-PA-DSS assessment services that may be offered by PA-QSAs. None of these services are required or recommended by PCI SSC. If these services are of interest to your company, please contact PA-QSAs for availability and pricing. Examples of non-PA-DSS assessment services include:

- Guidance on designing payment applications in accordance with PA-DSS
- Review of a software vendor’s software design, response to questions via e-mail or phone, and participation in conference calls to clarify requirements
- Guidance on preparing the *PA-DSS Implementation Guide*
- Pre-assessment (“gap” analysis) services prior to beginning formal PA-DSS assessment

- Guidance for bringing the payment application into compliance with PA-DSS if gaps or areas of non-compliance are noted during the assessment

Please Note: *When arranging for non-PA-DSS assessment services with a PA-QSA, care should be taken by both the vendor and the PA-QSA to ensure that the PA-QSA is not put in a position where it is required to assess its own work product as part of the actual PA-DSS assessment. Conflicts of interest may cause a payment application assessment to be rejected by PCI SSC.*

3.7 Technical Support throughout Testing

It is recommended that the vendor makes available a technical resource person to assist with any questions that may arise during the assessment. During the review, and to expedite the process, a vendor contact should be "on call" to discuss issues and respond to questions from the PA-QSA.

3.8 PA-DSS Vendor Release Agreement

The vendor's signed *Vendor Release Agreement* should be provided to the PA-QSA along with the payment application and other documents and materials at the beginning of the PA-QSA assessment process, and must be provided to PCI SSC by the PA-QSA along with the initial ROV submitted to PCI SSC. Among other things, the Vendor Release Agreement covers confidentiality issues, the vendor's agreement to PA-DSS Program requirements, policies and procedures, and gives the vendor's permission to the PA-QSA to release ROVs and related materials to PCI SSC for review. The vendor's signed PA-DSS VRA **must be delivered directly** to PCI SSC by the PA-QSA, along with the corresponding ROV.

It should be noted that a ROV cannot be reviewed by the PCI SSC without a current PA-DSS VRA on file from the relevant vendor.

So long as a current PA-DSS VRA is on file with the PCI SSC for the relevant vendor, it is not required to re-submit the PA-DSS VRA with each subsequent ROV.

3.9 The Portal

All documents relating to the payment application validation process are to be submitted by PA-QSAs, on behalf of the vendor, to the Council through the PCI SSC's secure web portal ("Portal").

The Portal maintains a first-in-first-out order to all submissions while they await review by the Council. Should a new submission be intended as a replacement for a previous version of a Validated Payment Application with known vulnerabilities, the Portal allows such submissions to be brought forward for immediate review.

The Portal is also used by the Council to track all communications relating to a particular submission.

3.10 PA-DSS Payment Application Acceptance Fees

All fees and dates for the PA-QSA's PA-DSS assessment are negotiated between the PA-QSA and the payment application vendor, and the vendor pays all such fees directly to the PA-QSA.

Vendors are also required to pay a *PA-DSS Payment Application Acceptance Fee* (all PA-DSS Program Fees are posted on the PCI SSC website) to PCI SSC immediately prior to Acceptance of each new payment application. For each new payment application, the *PA-DSS Payment Application Acceptance Fee* will be invoiced immediately prior to Acceptance, and must be received by PCI SSC for the application to be Accepted and added to the PCI SSC's List of Validated Payment Applications. Upon Acceptance, the PCI SSC will sign and return a copy of the Attestation of Validation to both the vendor and the PA-QSA.

There are no annual recurring PCI SSC fees associated with the Acceptance of a PA-DSS Validated Payment Application. There are, however, PCI SSC fees associated with vendor updates to PA-DSS Validated Payment Applications. Please see the section on *Validation Maintenance Fees* for more information.

Note:

The vendor pays all PA-QSA assessment related fees directly to the PA-QSA (these fees are negotiated between the vendor and the PA-QSA).

PCI SSC will bill the vendor for all PA-DSS Payment Application Acceptance Fees and the vendor will pay these fees directly to PCI SSC.

All PA-DSS Program fees are non-refundable and are subject to change upon posting of revised fees on the PCI SSC website.

4 Vendor Considerations – Managing a Validated Payment Application

4.1 Annual Revalidation

Annually, by the revalidation date noted on the List of Validated Payment Applications, the software vendor is **required** to submit an updated *Attestation of Validation,* performing the "Annual Revalidation" steps (as indicated in Part 2).

This annual process has been adopted to encourage software vendors to not only reaffirm that there have been no updates to the PA-DSS Validated Payment Application (if applicable), but also to encourage vendors to periodically consider whether updates to the PA-DSS Validated Payment Application are necessary to address changes to the external threat environment in which the payment application operates. If changes to the threat environment do necessitate changes to the payment application, the product should be updated accordingly and reassessed by a PA-QSA, preferably the PA-QSA that originally validated the payment application for PA-DSS compliance.

If an updated Attestation of Validation is not submitted for a listed payment application, that application will be deemed to have suffered an early administrative expiry. As such, the "Deployment Notes" on the List of Validated Applications will be amended to identify that the payment application is "Only acceptable for pre-existing deployments."

As there are no specific fees associated with Annual Revalidations, the PCI SSC will upon receipt of the updated Attestation of Validation: (i) review the submission for completeness; (ii) once completeness is established, update the List of Validated Payment Applications with the new revalidation date; and (iii) sign and return a copy of the updated Attestation of Validation to both the software vendor and the PA-QSA.

The process flow for annual revalidation is detailed in Figure 3.

4.2 Changes to Listed Payment Applications

Vendors update previously listed payment applications for various reasons—for example, adding auxiliary functionality or upgrading the baseline or core application.

From a PA-DSS perspective, there are essentially three types of change scenarios:

1. **No-Impact Changes** are minor changes (either administrative or software) made to a listed payment application that have no impact on the PA-DSS requirements. In this case, for the new version to be listed, the software vendor documents the change for the PA-QSA's review—see the *No-Impact Changes* section for specifics. Examples of minor updates include, but are not limited to, corporate identity changes or software changes to a graphical user interface or to supporting modules that perform no payment application functions.
2. **Low-Impact Changes** are minor changes made to a listed payment application that touch upon PA-DSS related functions of the payment application and have limited impact on the PA-DSS requirements. In this case, for the new version to be accepted, the software vendor submits the new version of the payment application for a partial or "delta" review – see *Low-Impact Changes* section for specifics.
3. **High-Impact Changes** - are changes made to a listed payment application that affect the PA-DSS related functions of the payment application and have a high impact on the PA-DSS

requirements. In this case, for the new version to be listed, the software vendor submits the new version of the payment application for a full PA-DSS review - see *High-Impact Changes* section for specifics. Examples of major updates include any changes that impact or change the functionality for PA-DSS requirements or impact the security functioning of the payment application in a way that cannot be considered minor; including but not limited to, how the application stores, processes, or transmits PAN or sensitive authentication data, how users are authenticated, how PAN is rendered unreadable for storage or transmission, how logs are generated and managed, use of remote access, use of wireless technology, or changes to application infrastructure.

In such cases where updates are made to previously listed applications and the vendor desires that the updated payment application information is reflected on the List of Validated Payment Applications, the vendor must submit the details of those changes to the PA-QSA, preferably to the PA-QSA that originally reviewed the payment application.

The PA-QSA then determines whether a full or partial re-assessment of the payment application is required. This decision is based on the degree to which the changes made to the application impact the security of the application, and/or the scope or depth of the changes being made. For example, the change may only impact auxiliary functionality and does not impact the core payment application.

If a listed payment application has undergone changes that may potentially affect PA-DSS requirements, and/or if the vendor wants the information in its *Attestation of Validation* and/or on the PCI SSC website revised, the vendor must submit proper change documentation to the PA-QSA to determine whether a full evaluation needs to be performed.

Note:

Minor Changes (No-Impact or Low Impact) are only permissible to previously listed payment applications that have yet to expire.

Modularization of payment functionality may help to minimize re-evaluations due to changes that do not impact payment functionality and security.

The sections below provide information on the supporting documentation that must be generated and the processes that are to be followed in order to successfully effect changes to the validation of a previously listed application.

The process flow for changes to listed applications is detailed in Figure 4.

4.2.1 Change Documentation

4.2.1.1 Vendor Change Analysis Document

All No-Impact and Low-Impact Changes (collectively referred to as “Minor Changes”) to PA-DSS Validated Payment Applications must be disclosed by the software vendor in a *Vendor Change Analysis* document. The *Vendor Change Analysis* submitted by the software vendor to the PA-QSA should contain the following information at a minimum:

- Name of the payment application;
- Payment application version number;
- Related payment application name and version number currently on the List of Validated Payment Applications;
- Description of the change;
- Indication of whether this is a *No-Impact Change* or a *Low-Impact Change* (see below);

- Description of why the change is necessary;
- Details of whether cardholder data and payment functions are impacted and what the impact is;
- Description of how the change functions;
- Description of testing performed by vendor to validate that PA-DSS security requirements are not negatively impacted;
- Explanation of how and why PA-DSS requirements are not negatively impacted;
- Description of how this change fits into vendor's versioning methodology, including how this version number indicates that this is a "minor" change;
- If applicable, description of use of programming practices/module approaches and how such use prevents a negative impact to requirements; and
- The Vendor's updated PA-DSS Implementation Guide.

4.2.1.2 PA-QSA Change Impact Document

All minor changes to PA-DSS Validated Payment Applications that the PA-QSA has determined to be *Low-Impact Changes* (see below) must be documented by the PA-QSA in a *PA-QSA Change Impact* document. Each *PA-QSA Change Impact* document must then be submitted by the PA-QSA to PCI SSC and must include the following:

- A high-level description of each change that has been made to the Validated Payment Application
- Citations of:
    - The original ROV that and any subsequent Minor Changes (including No-Impact and Low-Impact Changes) upon which the current Minor Change is based; and
    - Any supporting documentation used to substantiate the findings represented in the *Vendor Change Analysis*;
- A table that depicts the following information about every change that is embodied in the Minor Change to the Validated Payment Application from the previously approved version:
    - A description of the change;
    - Identification of the amended configuration item or items (system files, modules, etc.) that is/are impacted by the change;
    - A high-level assessment by the PA-QSA of the security impact of the change;
    - Identification of the PA-DSS requirements or test procedures that are impacted by the change;
    - Indication whether or not the impacted PA-DSS requirements necessitated an update to the ROV (the "Redline" ROV would have the detail of the changes); and
    - A high-level description of the testing completed, if any, used to validated the assessment;

4.2.2 No-Impact Changes

4.2.2.1 Vendor Change Analysis & PA-QSA Concurrence is Required

There are two types of No-Impact Changes:

- **Administrative Changes** – are limited to updates where no application changes have occurred but the vendor wishes to request a change to the way their application is currently listed. Administrative changes include, but are not limited to, changes to the application name or corporate entity name changes.
- **Payment Application Changes** – includes revisions to previously listed payment application, but that revision is deemed to have no impact on PA-DSS requirements.

In both cases, the software vendor prepares documentation of the change (a "*Vendor Change Analysis*") and submits the *Vendor Change Analysis* to the PA-QSA for review. It is *strongly recommended* that the vendor submit the *Vendor Change Analysis* to the same PA-QSA used for the original assessment.

If the PA-QSA agrees that the change as documented in the *Vendor Change Analysis* by the vendor has no impact on the PA-DSS related functions of the payment application:

(i) The PA-QSA must so notify the software vendor;

(ii) The vendor prepares and signs an *Attestation of Validation*, and sends it to the PA-QSA;

(iii) The PA-QSA signs their concurrence on the *Attestation of Validation* and forwards it, along with the *Vendor Change Analysis* and the payment application's updated PA-DSS Implementation Guide, to PCI SSC; and

(iv) PCI SSC will then review the *Attestation of Validation* and *Vendor Change Analysis* for quality assurance purposes.

If the PA-QSA does not agree with the vendor that the change, as documented in the *Vendor Change Analysis*, has no impact on the PA-DSS related functions of the payment application, the PA-QSA should return the *Vendor Change Analysis* to the vendor and work with the vendor to consider what actions are necessary to address the PA-QSA's observations.

Following successful PCI SSC quality assurance review of a No-Impact Change:

- An invoice for the applicable *No-Impact Change Fee* will be issued to the vendor.
- Upon payment of the invoice to PCI SSC as described in *Validation Maintenance Fees* below, the PCI SSC will: (i) amend the List of PA-DSS Validated Payment Applications on the PCI SSC website accordingly with the new information and (ii) sign and return a copy of the *PA-DSS Attestation of Validation* to both the software vendor and the PA-QSA. The expiry date of this newly listed application and version number will be the same as that of the "parent" payment application.

For quality issues associated any aspect of the submission, PCI SSC communicates those issues to the PA-QSA, and those issues are resolved according to the process depicted in Figure 2. PCI SSC reserves the right to reject any *Vendor Change Analysis* if it determines that a change described therein and purported to be a No-Impact Change by the PA-QSA or vendor is ineligible for treatment as a No-Impact Change.

4.2.3 Low-Impact Changes

4.2.3.1 PA-QSA Change Impact Document and a "Delta" Review are Required

If a previously listed payment application is revised, but that revision is deemed to have a low impact on PA-DSS requirements, then the software vendor prepares documentation of the change and submits the *Vendor Change Analysis* to the PA-QSA for review. It is *strongly recommended* that the vendor submit the *Vendor Change Analysis* to the same PA-QSA used for the original assessment.

Low-Impact Changes are expressly limited to the following specific types of changes to PA-DSS related functions of a Validated Payment Application:

1. Inclusion of minor updates or patches to validated OS versions upon which the payment application was previously validated;
2. Inclusion of minor updates or patches to supported 3rd party databases with which the payment application was previously validated;
3. Updates to reporting modules;
4. Additions or deletions of supported payment processors;
5. Inclusion of minor updates or patches to supported middleware with which the payment application was previously validated; and
6. Recompilation of unchanged code base with either the same compiler using different flags or with a completely different compiler.

Except for the specific types of changes identified immediately above, all other changes that have an impact on PA-DSS related functions of a Validated Payment Application are deemed to be High-Impact Changes and must be assessed by a PA-QSA through a full review.

In addition to the limitation detailed above, on the specific types of changes that may be considered by Vendors and PA-QSAs as Low-Impact Changes, there are critical requirements for the protection of cardholder data within PA-DSS that, if impacted by a change, are deemed to be High-Impact Changes and, accordingly, necessitate a full review of the amended payment application. The critical requirements of the PA-DSS that result in changes being automatically classified as High-Impact include the following areas:

- Sensitive Authentication Data;
- Remote Access;
- Default Passwords; and
- Protection of Stored PAN.

A list of the specific critical PA-DSS requirements, that if impacted necessitate a full review, is maintained in the table of Critical Test Procedures in the *ROV Reporting Instructions* document.

If the PA-QSA agrees that the change as documented in the *Vendor Change Analysis* by the vendor only have a low impact on PA-DSS requirements (based on the PA-QSA's review of the criteria above):

(i) The PA-QSA must so notify the software vendor;

(ii) The PA-QSA must perform an assessment of the PA-DSS requirements affected by the Low-Impact Change and produces a *PA-QSA Change Impact* document and make "redline" changes to the original ROV as appropriate;

(iii) The vendor prepares and signs an Attestation of Validation, and sends it to the PA-QSA;

(iv) The PA-QSA signs their concurrence on the *Attestation of Validation* and forwards it, along with the "Redline" version of the ROV, the payment application's updated PA-DSS Implementation Guide, and the *PA-QSA Change Impact* document, to PCI SSC; and

(v) PCI SSC will then review the Attestation of Validation, the “Redline” version of the ROV and the *PA-QSA Change Impact* document for quality assurance purposes.

If the PA-QSA does not agree with the vendor that the change, as documented in the *Vendor Change Analysis*, has only a low impact on the PA-DSS related functions of the payment application, the PA-QSA should return the *Vendor Change Analysis* to the vendor and work with the vendor to consider what actions are necessary to address the PA-QSA’s observations.

Following successful PCI SSC quality assurance review of a Low-Impact Change:

- An invoice for the *Low-Impact Change Fee* will be issued to the vendor.
- Upon payment of the invoice to PCI SSC as described in *Validation Maintenance Fees* below, PCI SSC will: (i) amend the List of PA-DSS Validated Payment Applications on the PCI SSC website accordingly with the new information; and (ii) sign and return a copy of the *Attestation of Validation* to both the software vendor and the PA-QSA. The expiry date of this newly listed application and version number will be the same as that of the “parent” payment application.

For quality issues associated any aspect of the submission, PCI SSC communicates those issues to the PA-QSA, and those issues are resolved according to the process depicted in Figure 2. PCI SSC reserves the right to reject any *PA-QSA Change Impact* document if it determines that a change described therein and purported to be a Low-Impact Change by the PA-QSA or vendor is ineligible for treatment as a Low-Impact Change.

4.2.4 High-Impact Changes

4.2.4.1 New PA-DSS Review is Required

If changes to the payment application do impact PA-DSS requirements and are ineligible for treatment as a *Low-Impact Change*, the payment application must undergo another full PA-DSS assessment. The PA-QSA will then submit a new ROV to the PCI SSC for Acceptance. In this situation, the vendor may first submit documentation of the change to the PA-QSA, who will determine whether the nature of the change impacts payment application security in accordance with current PA-DSS requirements.

4.3 Renewing Expired Applications

As an application approaches its expiration date, PCI SSC will notify the vendor of the pending expiration. The two options available for vendor consideration are full review or expiry:

1. <u>Full Review</u>: If the vendor intends to continue to sell the application. If so, the vendor contacts a PA-QSA and has the payment application fully re-evaluated against the then current version of the PA-DSS. It is not possible to use the Minor Change process to achieve this goal.
2. <u>Expiry</u>: In all other situations (e.g. the vendor indicates that it does not intend to continue selling the application or has gone out of business, or otherwise fails to submit the application for full re-assessment by the expiration date), PCI SSC will change the listed status of the payment application to “Only acceptable for **pre-existing** deployments” after the expiration date. This provides assurance to those already using the payment application that the application is compliant.

Note that if the vendor chooses to continue selling the application, once the application successfully passes through the PA-DSS assessment process again, it retains its status on the List of Validated Applications as “Acceptable for new deployments” and is assigned a new expiration date.

The process flow for renewing expired applications is detailed in Figure 4.

4.4 Validation Maintenance Fees

All fees and dates related to the PA-QSA's PA-DSS assessment of validated payment applications for the purposes of renewal or application updates are negotiated between the PA-QSA and the payment application vendor, and the vendor pays all fees directly to the PA-QSA.

There is no PCI SSC fee associated with the processing of Annual Revalidations.

If a listed payment application is revised, but the revision is minor and does not impact PA-DSS requirements, the vendor is required to pay the applicable *No-Impact Change Fee* (all PA-DSS Program Fees are posted on the PCI SSC website) to PCI SSC immediately prior to Acceptance of each such change.

If a listed payment application is revised, but the revision is minor with only a low impact on PA-DSS requirements, the vendor is required to pay the applicable *Low-Impact Change Fee* (all PA-DSS Program Fees are posted on the PCI SSC website) to PCI SSC immediately prior to Acceptance of each such change.

Note that all types of Minor Changes will be added as a child of the parent application already on the List of Validated Payment Applications

For any Minor Change to a PA-DSS Validated Payment Application, the applicable fee will be invoiced immediately prior to Acceptance, and must be received by PCI SSC for the minor change to be Accepted and added to the PCI SSC's List of Validated Payment Applications. Upon Acceptance, the PCI SSC will sign and return a copy of the Attestation of Validation to both the vendor and the PA-QSA.

Note:

The vendor pays all PA-QSA assessment related fees directly to the PA-QSA (these fees are negotiated between the vendor and the PA-QSA).

PCI SSC will invoice the vendor for all Validation Maintenance Fees and the vendor will pay these fees directly to PCI SSC.

A parent application must already exist on the List of Validated Payment Applications and have yet to expire in order to have a minor update accepted and listed.

All PA-DSS Program fees are non-refundable and are subject to change upon posting of revised fees on the PCI SSC website.

4.5 Notification Following a Security Breach, Compromise, or Known or Suspected Vulnerability

Using the procedures described in this section, vendors must promptly notify PCI SSC upon becoming aware of any actual or suspected vulnerability, security compromise or breach of any of their own listed payment applications that jeopardizes or could reasonably be expected to jeopardize the security of cardholder data (each a "Security Issue").

4.5.1 Notification and Timing

Notwithstanding any other legal obligations the vendor may have, the vendor must promptly notify PCI SSC of any Security Issue relating to any of the vendor's listed payment applications.

The vendor must also provide prompt feedback about any potential impact (possible or actual) the breach or vulnerability has had, may have, or will have.

Note:

Notification must take place no later than 24 hours after the vendor first discovers the Security Issue.

4.5.2 Notification Format

The vendor's formal notification to PCI SSC must be in writing in accordance with the Vendor Release Agreement, and should be preceded by a phone call to the PCI SSC PA-DSS Program Manager.

4.5.3 Notification Details

As part of the vendor's initial notification to PCI SSC, the vendor must supply the PCI SSC PA-DSS Program Manager with all information available to the vendor regarding the Security Issue. Typically, this should include, but is not limited to:

- The number of compromised accounts (if known);
- Any reports detailing the security breach or compromise (Do not include any compromised entities' names);
- Any reports or evaluations performed to investigate the security breach or compromise (Do not include any compromised entities' names); and
- The exact nature of the payment application's vulnerability.

PCI SSC, as provided in the PA-DSS VRA, may share certain information as required to support or enable an evaluation of the Security Issue to be performed to mitigate or prevent further security breaches or compromises.

4.5.4 Actions following a Security Breach or Compromise

In the event of PCI SSC's being made aware of a Security Issue related to a PA-DSS Validated Payment Application, PCI SSC may take the following actions:

- Notify all payment brands that a Security Issue has occurred.
- Attempt to obtain the forensics report to evaluate exactly how the Security Issue occurred.
- Communicate with the vendor of the application in question about the Security Issue and, where possible, share information relating to the Security Issue.
- Support the vendor's efforts to try and mitigate or prevent further Security Issues.
- Support the vendor's efforts to 1) correct any Security Issues, and 2) produce a guideline document to be issued to that vendor's customers, informing them of any potential vulnerability and detailing what actions should be taken in order to mitigate or prevent further Security Issues.
- Work with appropriate law enforcement agencies to help mitigate or prevent further Security Issues.
- Support and/or enable evaluations of the compromised payment application either internally or under the terms of the PA-DSS VRA, using PFIs to identify the cause of the compromise.

4.5.5 Withdrawal of Acceptance

PCI SSC reserves the right to suspend, withdraw revoke, cancel or place conditions upon its Acceptance of (and accordingly, remove from the *List of PA-DSS Validated Payment Applications*) any listed payment application in accordance with the PA-DSS VRA, including but not limited to, when it is clear that the payment application does not offer sufficient protection against current threats and does not conform to PA-DSS requirements, when the continued Acceptance of the payment application represents a significant and imminent security threat to its users, or if PCI SSC determines that the payment application has application Security Issue.

5 PA-QSA Reporting Considerations

5.1 PA-DSS Report Acceptance Process Overview

The PA-QSA performs the payment application review according to the *PA-DSS Security Assessment Procedures*, and produces a ROV that is shared with the vendor. If the ROV has all items "in place," then the PA-QSA submits the ROV and the vendor's signed PA-DSS VRA to PCI SSC. If the ROV does not have all items "in place," then the vendor must address those items highlighted in the ROV. For example, this may include updating user documentation or updating the software. Once the PA-QSA is satisfied that all documented issues have been resolved by the vendor, the PA-QSA submits the ROV and the vendor's then signed PA-DSS VRA to PCI SSC.

Note:

All ROVs and other materials must be submitted to PCI SSC in English or with certified English translation.

PCI SSC receives the ROV and reviews it from a quality assurance perspective. If the ROV meets all applicable quality assurance requirements (as documented in the QSA Qualification Requirements and related PA-DSS Program materials), and the vendor has paid the applicable Acceptance or Minor Change fee for the corresponding application, then PCI SSC sends a PA-DSS *Attestation of Validation*, countersigned by the PCI SSC, to both the vendor and the PA-QSA, and the adds the application to the List of Validated Payment Applications. For quality issues associated with ROVs, PCI SSC communicates those issues with the PA-QSA. It is then the responsibility of the PA-QSA to resolve the issues with PCI SSC and/or the vendor, as applicable. Such issues may be limited to updating the ROV to reflect adequate documentation to support the PA-QSAs decisions. However, if the issues require that the PA-QSA perform more testing, then the PA-QSA must notify the vendor that re-testing is needed and schedule that testing with the vendor.

The process flow for ROV Acceptance and ROV Review Process are detailed in Figure 1 and 2 respectively.

5.2 Delivery of the ROV and Related Materials

All documents relating to the payment application validation process must be submitted by PA-QSAs, on behalf of the vendor, to the Council through the PCI SSC's secure website ("Portal"). Council staff pre-screen Portal submissions to ensure that all required documentation has been included and the basic submission criterion has been followed.

There must be consistency between the information in documents submitted for review via the portal and the 'Details' fields within the Portal. Common errors in submissions include inconsistent application names or contact information and incomplete or inconsistent documentation. Incomplete or inconsistent submissions may result in a significant delay in the processing of requests for listing and/or may not be accepted for review by the PCI SSC.

The Portal maintains a first-in-first-out order to all submissions while they await review by the Council. Should a new submission be intended as a replacement for a previous version of a Validated Payment Application with known vulnerabilities, the Portal allows such submissions to be brought forward for immediate review.

The Portal is also used by the Council to track all communications relating to a particular submission.

5.2.1 Access to the Portal

Once a PA-QSA Company has had their first employee successful complete the individual PA-QSA certification process, PCI SSC will send login credentials and instructions for use of the Portal to the company's Primary PA-QSA. Additional credentials can be requested by each company's Primary PQ-QSA through the PCI SSC's PA-DSS Program Manager. Portal credentials may be issued to any employee of a PA-QSA Company and are not limited to PA-QSAs.

5.2.2 New Applications

For all initial submissions to the PCI SSC, the PA-QSA must submit the following by uploading to the Portal:

- Vendor Release Agreement (VRA) signed by the Vendor
- ROVs completed in accordance with the ROV Reporting Instructions which contains the following information:
    - Executive Summary (Includes Reseller/Integrator List)
    - Requirements – Testing Procedures
    - Appendix B – Laboratory Confirmation
    - Attestation of Validation (AOV) signed by both the Vendor and the PA-QSA of Record
- Implementation Guide for the Payment Application assessed

5.2.3 Resubmissions

For subsequent reviews, if multiple iterations of a ROV are required before PCI SSC accepts an application; the PA-QSA must submit ROV versions that include tracking of cumulative changes within the document.

5.2.4 No-Impact Changes

For all submissions of a No-Impact Change to an already listed application, the PA-QSA must submit the following documents through the Portal.

- *Vendor Change Analysis* document;
- Updated PA-DSS Implementation Guide for the assessed payment application; and
- Attestation of Validation signed by both the Vendor and the PA-QSA.

5.2.5 Low-Impact Changes

For all submissions of a Low-Impact Change to an already listed application, the PA-QSA must submit the following documents through the Portal.

- PA-QSA's Change Impact document;
- Updated PA-DSS Implementation Guide for the assessed payment application;
- Updated ROV which contains the following:
    - Summary of requirements assessed and any resulting changes;
    - Updated Executive Summary and Requirement with edits clearly identified (i.e. "redlined"); and
    - Confirmation of Testing Laboratory (PA-DSS, Appendix B); and

- Attestation of Validation signed by both the Vendor and the PA-QSA.

5.3 PA-DSS Reporting Processes

PCI SSC will base Acceptance of a payment application primarily on the results documented in the ROV. Upon receipt of the ROV, the following will apply:

- PCI SSC shall review the ROV (generally within 30 calendar days of receipt) and determine if it is acceptable.
- If no issues or questions to the PA-QSA are identified, PCI SSC shall bill the vendor for the applicable Acceptance or Minor Update fee. Once the fee is received, PCI SSC will issue the *Attestation of Validation*, countersigned by PCI SSC, post the payment application and vendor's information to the PCI SSC website, and the application is thereby Accepted.
- If questions or issues are identified and sent to the PA-QSA, the process described above will restart upon receipt of a complete and acceptable revised ROV or response ("Revised ROV") from the PA-QSA. PCI SSC reserves the right to ask for additional supporting documentation that may be necessary to substantiate the findings documented in the ROV. The process re-start does not occur until receipt of an acceptable Revised ROV addressing all previously identified items. PCI SSC will generally review a Revised ROV within 30 calendar days of receipt.
- Should additional questions or issues arise, the cycle repeats until a satisfactory Revised ROV is received, at which time, subject to receipt of the applicable Acceptance or Minor Change fee, PCI SSC will issue the *Attestation of Validation*, post the information to the PCI SSC website, and the application is thereby Accepted. Additional issues or questions may be raised at any time prior to Acceptance.
- ROVs that have been returned to the PA-QSA for correction must be resubmitted to the PCI SSC within 30 days. If this is not possible, the PA-QSA must inform the PCI SSC of the timeline for response. Lack of response on ROVs returned to the PA-QSA for correction may result in the submission being closed. Submissions that have been closed will not be reopened and must be resubmitted as if they are new ROV submission.

For reports related to minor updates to existing listed application versions, based on the vendor's *Attestation of Validation*, the above PA-DSS ROV Acceptance process is the same, and PCI SSC shall issue a revised Attestation of Validation and post the revised information to the PCI SSC website unless issues or questions arise, in a manner similar to the aforementioned.

The listing on the List of Validated Payment Applications will contain, at minimum, the information specified below. Each characteristic is detailed in "*Appendix A: Application Elements for the Attestation of Validation and the List of Validated Payment Applications*."

- Payment Application Vendor
- Payment Application Identifier
  - Payment Application Name
  - Payment Application Version Number
  - Application Type
  - Target Market, if applicable
  - Reference Number
- Description Provided by Vendor

***Note**:*

PCI SSC will not grant any "partial approvals" based upon the ability of a payment application to meet some—but not all—of the requirements.

- Tested Platforms/Operating Systems
- Required dependencies
- Validation Notes (PABP or PA-DSS version)
- Deployment Notes
- Revalidation Date
- Expiry Date
- PA-QSA Company

5.4 Quality Assurance Program

PCI SSC reviews ROVs and PA-QSA performance for quality assurance purposes. As stated in the *QSA Validation Requirements* and the *PA-QSA Agreement*, PA-QSAs are required to meet all quality assurance standards set by PCI SSC. The various phases of the QA program are described below.

The process flow for the QA program is detailed in Figure 5.

5.4.1 Outcomes of an ROV Review

Quality assurance reviews of ROVs will result in one of the following outcomes:

- The payment application is determined to be ineligible for validation under the PA-DSS Program and the ROV will not be Accepted; or
- The payment application is determined to be eligible for Acceptance under the PA-DSS Program and therefore the ROV will be reviewed and determined to either:
    - Meet the requirements of the PA-DSS Program; or
    - Not meet the requirements of the PA-DSS Program in which case all identified issues with the ROV must be resolved before the ROV review can be completed.

5.4.1.1 Critical Test Procedures

PCI SSC places emphasis on “Critical Test Procedures (i.e. specific ROV testing procedures) that are considered critical to the protection of cardholder data in PA-DSS compliant payment applications. These areas have historically been targeted by attackers attempting to compromise payment applications. Critical Test Procedures cover areas such as; Sensitive Authentication Data, Remote Access, Default Passwords, Protection of Stored PAN, Logging and Wireless.

If any Critical Test Procedure is not properly addressed by the PA-QSA, the ROV under review will be returned for correction.

Details of the specific PA-DSS requirements that are to be considered as Critical Test Procedures are maintained in the *ROV Reporting Instructions*.

5.4.2 Types of ROV Reviews

The type of review done on a particular ROV submission is determined by the status of the PA-QSA Company (see section below on *PA-QSA Status*) and is variable at the discretion of the PCI SSC.

5.4.2.1 Pro Forma Reviews

This review focuses on the Executive Summary and Critical Test Procedures, and reduces the time a report is in queue with the Council. Only minimal feedback is provided to the PA-QSA.

5.4.2.2 Full Reviews

This review will examine all aspects of the ROV submission. The purpose is to ensure that PA-QSAs are given enhanced feedback and guidance.

5.4.2.3 Detailed Full Reviews with Work Papers

This review will examine all aspects of the ROV submission and the supporting documentation that was either provided to the PA-QSA by the application vendor or created by the PA-QSA as a result of the assessment process. The purpose is to establish confidence in the efforts taken by the PA-QSA to reach their opinion of the subject payment application and to provide enhanced feedback and guidance.

5.4.3 PA-QSA Audit Program

The purpose of the PA-QSA audit program is to ensure that the assessment process and overall quality of report submissions remains at a level that is consistent with the objectives of the PCI PA-DSS Program Guide.

Each calendar year all PA-QSA organizations submitting reports to the SSC are subject to an audit of their submissions.

The audit process is a more formalized method of review. The normal review practice (pro forma) is to evaluate the submission for completeness. The audit process however, is a more robust evaluation of the PA-QSA work. The audit will evaluate the work product of the PA-QSA for a set of reports. The audit process will encompass the report submissions, along with an evaluation of work papers and the PA-QSA's internal QA manual. This will help to ensure the organization's internal QA processes are being followed. Additionally, the PA-DSS Implementation Guide and/or other supporting documents pertaining to the payment application under audit will be reviewed. Finally, the PCI SSC may at its discretion conduct an onsite audit.

5.4.4 PA-QSA Status

The PA-QSA program recognizes five (5) quality status levels for PA-QSA companies. The quality status level of a PA-QSA Company is determined by the PCI SSC based on review of submissions and feedback from clients and/or payment brands.

These levels are not progressive, for example it is possible for a PA-QSA Company to move from "PA-QSA In Good Standing" to "Remediation" without being through "Oversight." A PA-QSA Company may even move directly from "PA-QSA In Good Standing" to "Revocation" if issues found with work quality are significant enough to warrant this.

At any of these status levels, PCI SSC may require an onsite visit with the PA-QSA Company to audit their internal QA program, at the expense of the PA-QSA Company.

Note that if a payment application included on the PCI SSC *List of PA-DSS Validated Payment Applications* is compromised due to PA-QSA error, then that PA-QSA may immediately be placed into Remediation.

The PA-QSA quality status levels used by the Council are as follows:

5.4.4.1 New PA-QSA

When a PA-QSA Company joins the PA-DSS program, the PCI SSC will provide support to ensure the quality expectations of the PCI SSC are understood and being met by the PA-QSA Company. A New PA-QSA Company will usually have full reviews completed on their ROV submissions. They will be asked to submit their internal Quality Manual to the PCI SSC for review and may also be asked to submit other documentation such as work papers for some or all of their ROV submissions.

When the Council has reviewed several ROV submissions (typically 3 to 5) from the new PA-QSA Company and quality expectations are being met, the PA-QSA Company status will move to “PA-QSA In Good Standing” status. If quality expectations are not met the PA-QSA Company status may be altered to Oversight, Remediation or even Revocation depending on the severity of the issues found.

There are no external indications on the PCI SSC website that a PA-QSA Company is in New PA-QSA status.

5.4.4.2 PA-QSA In Good Standing

This is the “normal” status, which most PA-QSA companies are expected to hold while participating in the PA-DSS program. A PA-QSA Company that is a “PA-QSA In Good Standing” with the PCI SSC will usually have Pro Forma reviews completed on their ROV submissions. As well as reviews of each submission, the overall quality of submissions, as a broader body of work, will be monitored by the PCI SSC to detect any deterioration of quality levels over time. In addition the PA-QSA Company will be subject to periodic audit by the PCI SSC.

5.4.4.3 Oversight

The PCI SSC may place a PA-QSA Company into Oversight if quality problems are detected. Oversight is a mandatory program; if the Council determines that Oversight is warranted the PA-QSA Company must participate if they wish to remain within the PA-DSS program. A PA-QSA Company that is in Oversight will usually have full reviews completed on their ROV submissions. They will be asked to submit their internal Quality Manual to the PCI SSC for review and may also be asked to submit other documentation such as work papers for some or all of their ROV submissions.

Additional detail is communicated to the PA-QSA Company as to what corrective actions need to be taken to improve the overall quality of submissions. The PA-QSA is required to develop and submit an Oversight action plan to the Council. This document will include information on ways the PA-QSA intends to rectify outstanding quality issues. Lessons learned throughout the Oversight program should be incorporated into the PA-QSAs future work product thereby showing significant improvement in quality.

Oversight should be completed within 90 days. Oversight may be extended only if the PA-QSA has been able to demonstrate positive progress. Failure to demonstrate improved quality may lead to remediation or revocation.

PCI SSC will charge a *Detailed ROV Review Fee* (see Appendix B) for all reports submitted and resubmitted during oversight.

There are no external indications on the PCI SSC website that a PA-QSA Company is in Oversight status.

5.4.4.4 Remediation

The PCI SSC may place a PA-QSA Company into Remediation if significant quality problems are detected. Remediation is a mandatory program; if the Council determines that Remediation is warranted the PA-QSA Company must participate if they wish to remain within the PA-DSS program. A PA-QSA Company that is in Remediation will typically have detailed full reviews completed on their ROV submissions. They will be asked to submit their Quality Manual to the PCI SSC for review and will be asked to submit other documentation such as work papers for some or all of their ROV submissions

The PA-QSA Company must also submit a remediation plan to PCI SSC detailing how the PA-QSA plans to improve quality of their reports.

Additional detail is communicated to the PA-QSA Company as to what corrective actions need to be taken to improve the overall quality of submissions and a member of the PCI SSC will provide support on a case management basis. A minimum of five (5) ROV submissions, each of which achieve the required levels of quality, are normally required for a PA-QSA Company to successfully complete Remediation. The PCI SSC will also require the PA-QSA Company to evidence the lessons learned in an updated Quality Manual.

If the PA-QSA Company makes sufficient improvement during the Remediation process their status will be altered to Oversight or "PA-QSA In Good Standing." If the PA-QSA Company fails to meet quality standards during remediation, then the PA-QSA enters into Revocation.

Remediation is expected to be completed within 90 days. In the event that the goals of the Remediation program cannot be achieved within this period, Remediation may be extended once by an additional 90 days, only if the PA-QSA has been able to demonstrate positive progress to the satisfaction of the PCI SSC.

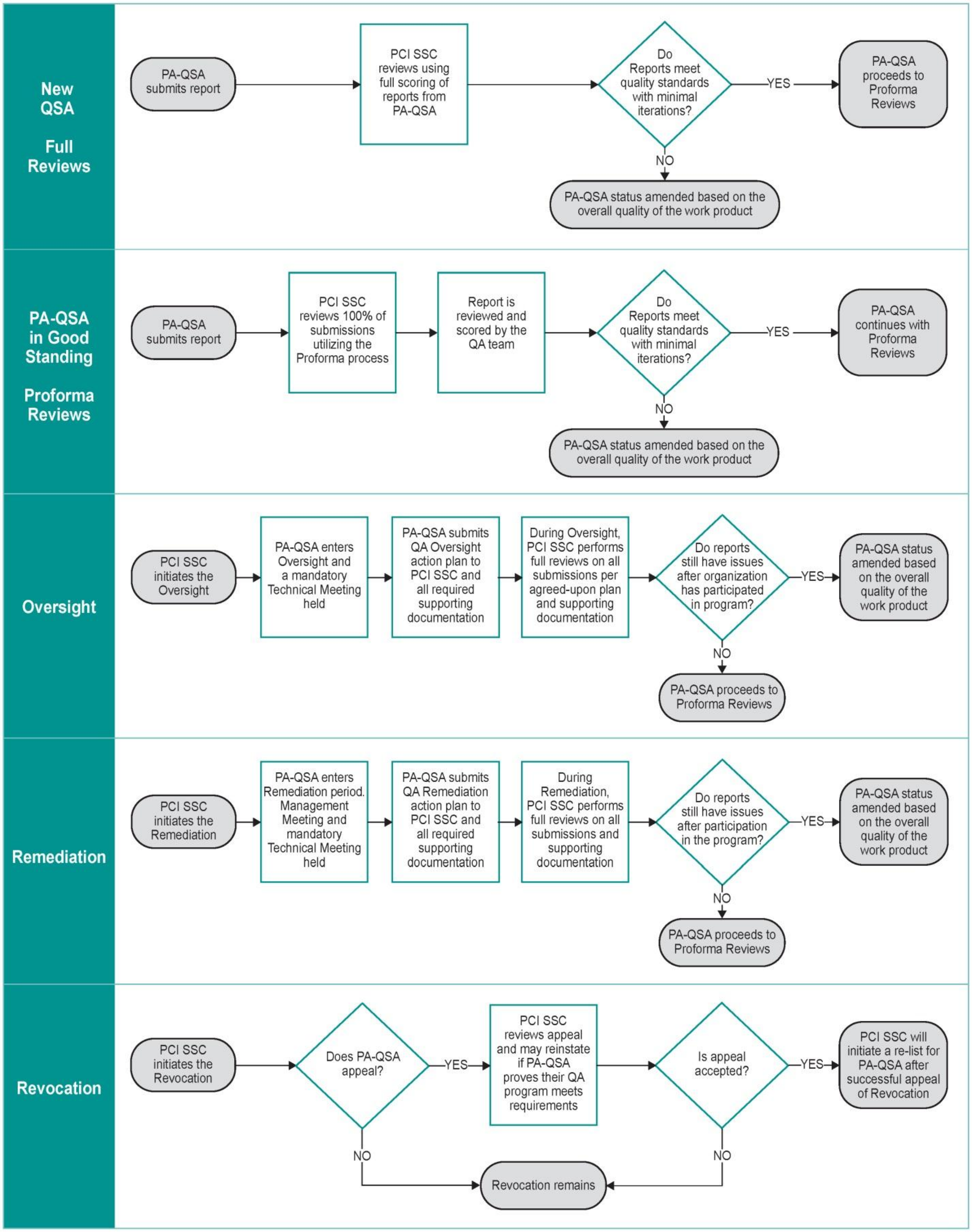
PCI SSC will charge a *PA-QSA Remediation Program Fee* for entry into the Remediation Program and a *Detailed ROV Review Fee* for all reports submitted and resubmitted during Remediation. See Appendix B for details of all applicable fees.

The PCI SSC website will be updated to show that the PA-QSA Company is in Remediation status.

5.4.4.5 Revocation

Serious quality problems may lead to a PA-QSA Company to be revoked from the PA-DSS program. When a PA-QSA qualification is revoked, the assessor is removed from the PCI SSC list of approved PA-QSAs and is no longer eligible to perform PA-QSA assessments, process ROVs, or otherwise participate in the PA-DSS Program; provided, that if and to the extent approved by PCI SSC in writing, the PA-QSA will be required to complete any PA-DSS assessments for which it was engaged prior to the effective date of the Revocation. The PA-QSA can appeal the Revocation, but unless otherwise approved by PCI SSC in writing in each instance, will not be permitted to perform PA-QSA assessments, process ROVs, or otherwise participate in the PA-DSS Program until it has demonstrated to PCI SSC's satisfaction that it meets all applicable QSA and PA-QSA requirements as documented in PA-QSA Qualification Requirements and supporting documents

5.5 Figure 5: PA-QSA QA Programs for Report Reviews


New QSA
Full Reviews
PA-QSA submits report
PCI SSC reviews using full scoring of reports from PA-QSA
Do Reports meet quality standards with minimal iterations?
YES
PA-QSA proceeds to Proforma Reviews
NO
PA-QSA status amended based on the overall quality of the work product
PA-QSA in Good Standing
Proforma Reviews
PA-QSA submits report
PCI SSC reviews 100% of submissions utilizing the Proforma process
Report is reviewed and scored by the QA team
Do Reports meet quality standards with minimal iterations?
YES
PA-QSA continues with Proforma Reviews
NO
PA-QSA status amended based on the overall quality of the work product
Oversight
PCI SSC initiates the Oversight
PA-QSA enters Oversight and a mandatory Technical Meeting held
PA-QSA submits QA Oversight action plan to PCI SSC and all required supporting documentation
During Oversight, PCI SSC performs full reviews on all submissions per agreed-upon plan and supporting documentation
Do reports still have issues after organization has participated in program?
YES
PA-QSA status amended based on the overall quality of the work product
NO
PA-QSA proceeds to Proforma Reviews
Remediation
PCI SSC initiates the Remediation
PA-QSA enters Remediation period. Management Meeting and mandatory Technical Meeting held
PA-QSA submits QA Remediation action plan to PCI SSC and all required supporting documentation
During Remediation, PCI SSC performs full reviews on all submissions and supporting documentation
Do reports still have issues after participation in the program?
YES
PA-QSA status amended based on the overall quality of the work product
NO
PA-QSA proceeds to Proforma Reviews
Revocation
PCI SSC initiates the Revocation
Does PA-QSA appeal?
YES
PCI SSC reviews appeal and may reinstate if PA-QSA proves their QA program meets requirements
Is appeal accepted?
YES
PCI SSC will initiate a re-list for PA-QSA after successful appeal of Revocation
NO
NO
Revocation remains

6 Legal Terms and Conditions

Acceptance of a given payment application by the PCI Security Standards Council LLC (PCI SSC) only applies to the specific version of that payment application that was reviewed by a PA-QSA and subsequently accepted by PCI SSC (the “Accepted Version”). If any aspect of a payment application or version thereof is different from that which was reviewed by the PA-QSA and Accepted by PCI SSC – even if the different payment application or version (the “Alternate Version”) conforms to the basic product description of the Accepted Version – then the Alternate Version should not be considered Accepted by PCI SSC, nor promoted as Accepted by PCI SSC.

No vendor or other third party may refer to a payment application as “PCI Approved,” or “PCI SSC Approved” nor otherwise state or imply that PCI SSC has, in whole or part, approved any aspect of a vendor or its payment applications, except that to the extent PCI SSC has issued an Attestation of Validation provided by PCI SSC. All other references to PCI SSC’s Acceptance or Approval of a payment application or version thereof are strictly and actively prohibited by PCI SSC.

PCI SSC Acceptance signifies that (i) a PA-QSA has determined that a payment application complies with the PA-DSS and therefore implements certain security and operational characteristics important to the achievement of PCI SSC’s goals and (ii) the corresponding ROV has successfully completed PCI SSC’s QA review, but such Acceptance does not under any circumstances include or imply any endorsement or warranty by PCI SSC or any payment brand regarding the payment application vendor or the functionality, quality, or performance of the payment application or any other product or service. PCI SSC does not warrant any products or services provided by third parties. PCI SSC Acceptance does not, under any circumstances, include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services that have been Accepted by PCI SSC, shall be provided by the party providing such products or services, and not by PCI SSC or any payment brands.

.

Appendix A: Elements for the Attestation of Validation and *List of Validated Payment Applications*

A.1 Payment Application Vendor

This entry denotes the **Payment Application Vendor** for the validated payment application.

A.2 Payment Application Identifier

The **Payment Application Identifier** is used by PCI SSC to denote relevant information for each validated payment application, consisting of the following fields (fields are explained in detail below):

- Payment Application Name
- Payment Application Version #
- Payment Application Type
- Target Market, if applicable
- Reference Number

Example of a Payment Application Identifier:

Component	Description
Application Name	Acme Payment 600
Application Version #	PCI 4.53
Application Type	POS Suite
Target Market	(None noted)
Reference #	09-01.00111.001

Payment Application Identifier: Detail

- **Payment Application Name**

  Payment Application Name is provided by the vendor, and is the name by which the payment application is sold.

- **Payment Application Version #**

  Payment Application Version # represents the specific application version reviewed in the PA-DSS assessment. The format is set by the vendor and may consist of a combination of fixed and variable alphanumeric characters.

> ***Note:***
>
> *In PA-DSS, see Instructions and Content for Report on Validation section for details about content to include in the PA-DSS ROV for vendor's versioning methods*.
>
> *Customers are strongly advised to purchase and deploy only those payment applications with the Application Version # whose characters match exactly the Application Version # shown on the List of Validated Payment Applications.*

- **Payment Application Type**

  The payment application type denotes the major categories of payment functions performed by payment applications, and consists of the following:

Type	Function	Description
01	POS Suite/General	Point of sale software which can be used by merchants for numerous payment channels, including face-to-face, mail-order/telephone order (MOTO, including call centers), Interactive Voice Response (IVR), Web (for manually entered e-commerce, MOTO, etc, transactions), and EFT/check authentication.
02	Payment Middleware	Payment software that facilitates transmission and/or processing of payment authorization and settlement from merchant POS to other merchant systems or to processors.
03	Payment Gateway/ Switch	Payment software sold or distributed to third parties to facilitate transmission and/or processing of payment authorization and settlement between merchant systems and processors.
04	Payment Back Office	Software that allows payment data to be used in "back office" locations, for example, for fraud reporting, marketing, hotel property management, or managing and reporting revenue. While these applications may not be part of authorization and settlement, often they are bundled with payment applications as software suites, and can be, but are not required to be, validated as part of a PA-DSS assessment.
05	POS Admin	Software that administers or manages POS applications.
06	POS Specialized	Point of sale software which can be used by merchants for specialized transmission methods, such as Bluetooth, Category 1 or 2 mobile, VOIP, etc.
07	POS Kiosk	Point of sale software for payment card transactions that occur in attended or unattended kiosks, for example, in parking lots.
08	POS Face-to-Face/POI	Point of sale software used by merchants solely for face-to-face or Point of Interaction (POI) payment card transactions. These applications may include middleware, front office or back office software, store management software, etc.
09	Shopping Cart & Store Front	Payment software for e-commerce merchants, where the consumer selects purchases from the Store Front and enters cardholder data in the Shopping Cart, and the Shopping Cart transmits and processes that cardholder data for authorization and settlement. This is different from the "Web" mentioned under POS Suite, where the merchant manually enters the data in a "virtual" POS for authorization and settlement.
10	Card-Not-Present	Payment software that is used by merchants to facilitate transmission and/or processing of payment authorization and/or settlement in card not present channels
11	Automated Fuel Dispenser	Payment software that provides operation and management of point of sale transactions, including processing and/or accounting functions in fuel dispensing environments

Type	Function	Description
12	Payment Module	Payment software that operates as a component of a broader application environment upon which it is dependent to operate. Such software must have distinguishable configuration identifiers that are easily discernible from the broader application environment.

- **Target Market, if applicable**

  The Target Market denotes a target market for the payment application. For example, the target market may be one of the following:

  - Retail
  - Processors
  - Gas/oil
  - E-commerce
  - Small/medium merchants

  Note:
  This is intended to indicate if the payment application is designed specifically for a certain market, not for software vendor marketing purposes.

- **Reference Number**

  PCI SSC assigns the Reference number once the application is posted to the Website; this number is unique per vendor and will remain the same for the life of the application's listing.

  An example reference number is 08-XX.XXXXX.XXX.AAA, consisting of the following:

Field	Format
Year of listing	2 digits + hyphen
Payment Application Type (see above)	2 digits + period
Vendor #	5 digits + period (assigned alphabetically initially, then as received)
Vendor App #	3 digits + period (assigned as received)
Minor version	3 alpha characters (assigned as received)

A.3 Description Provided by Vendor

This section allows for the submission of a description of the payment application that is to be used in the List of Validated Payment Application should the ROV be accepted. All descriptions must be acceptable to PCI SSC and the Council reserves the right to modify any description based on the review of the ROV.

A.4 Tested Platforms/Operating Systems

Identify the specific operating system type and version and any other platform components that the application was tested on.

A.5 Required Dependencies

Identify specific dependencies that the submitted payment application has to other PA-DSS Validated Payment Applications, Approved Point of Interaction Devices, other hardware environments, or broader software environments. Such dependencies must include specific version/firmware and/or hardware identifiers and any relevant PCI PA-DSS or PTS reference numbers.

As much as any payment application may have required dependencies, some of the Payment Application Types defined above (for example POS Face-to-Face/POI and Payment Module) are expected to have defined dependencies.

A.6 Validation Notes

Validation Notes are used by PCI SSC to denote what standard, and the specific version thereof, was used to assess the compliance of a Validated Payment Application. Please see table under “Expiry Date” below for examples.

A.7 Deployment Notes

Deployment Notes are used by PCI SSC to denote the scenarios in which Validated Payment Applications are recommended for use. Assigned deployment notes are determined by the vendor’s active participation in annual re-validation, whether or not the particular version of the payment application is still being supported by the vendor, or by the payment application’s Expiration Date (noted below).

Validated Payment Applications are denoted with one of the following Deployment Notes:

- **Acceptable for new deployment** – All newly Accepted PA-DSS Validated Payment Applications are initially put into this state and will maintain this state until such time that (i) annual revalidation requirements are not maintained by the vendor causing an administrative early expiry, or (ii) the Validated Payment Application expires as a matter of course based on the version of the PA-DSS under which it was validated.
- **Only acceptable for pre-existing deployments** – This deployment note is assigned to Validated Payment Applications where either (i) annual revalidation requirements are not maintained by the vendor causing an administrative early expiry, or (ii) the Validated Payment Application expires as a matter of course based on the version of the PA-DSS under which it was validated. Validated Payment Applications that have expired should not be purchased for new implementations but may continue to be used on systems where they were previously deployed.

These deployment notes are used by the Council to note the status of a Validated Payment Application is relation to its Expiry Date. Please refer to any specific brand requirements for usage of Validated Payment Applications.

Please see table under Expiry Date below for examples.

A.8 Revalidation Date

The **Revalidation Date** is used by PCI SSC to indicate when the software vendor’s annual *Attestation of Validation* is due. The Annual Revalidation is part of the *Attestation of Validation* form.

A.9 Expiry Date

The **Expiry Date** for PA-DSS Validated Payment Applications is the date by which a vendor must get the application re-evaluated against the current PA-DSS requirements in order to maintain the acceptance. The Expiry Date is related to the Deployment Notes, noted above.

PCI SSC will endeavor to update the PA-DSS on a 36-month cycle, in conjunction with updates to PCI DSS. Acceptance for PA-DSS validated payment applications expires three years past the effective date of a subsequent update of the PA-DSS requirements. The objective is a three -year minimum approval life expectancy, barring a severe threat that may require immediate changes.

For example: Payment applications validated against PA-DSS Version 2.0 will have an expiration date of 2016 as the next PA-DSS version is expected to be released in October 2013; while reviews against PA-DSS Versions 1.2 will expire in October 2013.

There is currently no sunset date for PA-DSS Validated Payment Applications that were on the List of Validated Payment Applications at the time of deployment. Deployed payment applications that expire may continue to be used. The expiration timeframe is associated with new purchases/deployments, not existing deployments.

Validation Notes	Expiry Date	Deployment Notes	Annual Revalidation Required
Validated According to PA-DSS (PA-DSS v2.0)	28 October 2016	Acceptable for New Deployments	Yes
Validated According to PA-DSS (PA-DSS v1.2.1, v1.2, or v1.1)	28 October 2013	Acceptable for New Deployments	Yes
Validated According to PABP (PABP 1.4)	2 March 2011	Only acceptable for pre-existing deployments	No
Validated According to PABP (PABP 1.3)	2 June 2010	Only acceptable for pre-existing deployments	No
Pre-PCI Application (Prior to PABP 1.3)	2 December 2009	Only acceptable for pre-existing deployments	No

A.10 PA-QSA Company

This entry denotes the name of the **Payment Application Qualified Security Assessor Company** that performed the validation and determined that the payment application is compliant with PA-DSS.

Appendix B: Identification of Certified Payment Application Builds

Note: *For future consideration*

While certified payment application builds are not a requirement at this time, we encourage software vendors and PA-QSAs to work together to develop methods to certify and digitally sign payment application builds. PCI SSC reserves the right to require certified application builds in the future.

For example, such a method could include the following:

Vendors clearly identify a certified build for general release. Ideally, a build certified by a PA-QSA as PA-DSS compliant should be fingerprinted—digitally signed (code-signed)—by both the software vendor and the QSA when packaged for delivery. At the very least, the delivery should be identified unambiguously by name, version, build number, and date-time stamp, and verifiable with an MD5 digest and corresponding build header. In this manner, PA-DSS requirement 7.2 for delivery assurance via "known chain-of-trust" is strengthened. Also, this could also help support a Payment Brand related PA-DSS programs, and help foster customer awareness and confidence.