Payment Card Industry (PCI)

Payment Application Data Security Standard (PA-DSS) v3.0

Program Guide

Version 3.0

February 2014

Document Changes

Date	Version	Description
October 1, 2008	1.2	To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
July 2009	1.2.1	To align content with new PCI DSS v1.2.1 and to implement minor changes noted since original v1.2.
January 2012	2.0	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.
February 2014	3.0	▪ Harmonization with other Program documents and general clarification to align content with PA-DSS v3.0 ▪ Process diagrams updated to reflect updates to respective processes ▪ Added section and Appendix B for wildcard versioning ▪ Former Appendix B changed to Appendix C (Identification of Certified Payment Application Builds) ▪ Updated criteria and process for delta assessments ▪ Updated section on Payment Application change types ▪ "Change Documentation" section added to clarify process requirements ▪ Changed "Quality Assurance Program" section to "Assessor Quality Management Program" and updated processes accordingly ▪ Clarified PA-QSA Company laboratory requirements ▪ Added Appendix D: PA-QSA Change Impact

Table of Contents

1 Introduction

This document provides an overview of the PCI SSC Payment Application Data Security Standard program ("PA-DSS Program") operated and managed by the PCI Security Standards Council, LLC ("PCI SSC"), and should be read in conjunction with the *PA-QSA Qualification Requirements* as well as those documents referenced in Section 1.2, "Related Publications," below. This section describes the following:

- Program Background
- Program Roles and Responsibilities
- Program Overview
- Preparation for the Review
- Reporting Considerations
- Post-Validation Activities
- Assessor Quality Management Program

1.1 Program Background

In response to requests from merchants and other members of the Payment Card Industry (PCI) for a unified set of payment account data security requirements, PCI SSC has adopted and maintains the *PCI Data Security Standard* (PCI DSS), a set of requirements for cardholder data protection across the entire industry, the current version of which is available on the PCI SSC website (Website). Key to the success of the PCI DSS is merchant and service provider compliance. When implemented appropriately, PCI DSS Requirements provide rigorous defense against data exposure and compromise. Ensuring Payment Applications meet PCI DSS Requirements and are installed into merchant or service-provider environments in a manner that supports PCI DSS compliance is important to the effectiveness of the Program.

To help merchants and service providers achieve this goal, PCI SSC manages the Program. The Program promotes the development, implementation and maintenance of secure Payment Applications that help support compliance with the PCI DSS.

Organizations qualified by PCI SSC to validate PA-DSS Payment Applications on behalf of Vendors are referred to as Payment Application Qualified Security Assessor Companies (PA-QSA Companies), further described below. The quality, reliability, and consistency of a PA-QSA Company's work provide confidence that the application has been validated for PA-DSS compliance.

1.2 Related Publications

The *PA-DSS Program Guide* should be used in conjunction with the latest versions of the following PCI SSC publications, each as available through the Website:

Document name	Description
PCI Payment Application Data Security Standard – Requirements and Security Assessment Procedures ("PA-DSS")	The PA-DSS and the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* list and define the specific technical requirements and provide the assessment procedures used by PA-QSA Companies to validate the Payment Application's compliance.

Document name	Description
PCI Report on Validation Reporting Template for PA-DSS ("ROV Reporting Template")	The ROV Reporting Template is mandatory for completing a Report on Validation and includes detail on how to document the findings of a PA-DSS Assessment.
Payment Application Data Security Standard (PA-DSS) Attestation of Validation ("AOV")	AOV is a form for PA-QSA Companies to attest to the results of a PA-DSS Assessment, as documented in the PA-DSS Report on Validation.
Payment Card Industry (PCI) Data Security Standard Qualification Requirements for Qualified Security Assessors (QSAs) ("QSA Qualification Requirements"); and *Payment Card Industry (PCI) Qualification Requirements for Payment Application Qualified Security Assessors (PA-QSAs)* ("PA-QSA Qualification Requirements")	The *QSA Qualification Requirements* and *PA-QSA Qualification Requirements* together define the baseline set of requirements that must be met by a PA-QSA Company and QSA Employees in order to perform PA-DSS Assessments.
Vendor Release Agreement ("VRA")	The VRA establishes the terms and conditions under which validated Payment Applications are accepted and listed by PCI SSC.

The most current versions of 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")

1.3 Updates to Documents and Security Requirements

It is necessary to regularly review, update and improve the security requirements used to evaluate Payment Applications. Therefore, PCI SSC endeavors to publish updates to its Payment Application security requirements every three years. 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 changes are required, PCI SSC will endeavor to work closely with PCI SSC's community of Participating Organizations and Vendors to help minimize the impact of any changes.

1.4 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 Company; (ii) received the fee and all documentation required with respect to the Payment Application as part of the Program; (iii) confirmed that the ROV is correct as to form, the PA-QSA Company properly determined that the Payment Application is eligible to be a PA-DSS Validated Payment Application, the PA-QSA Company adequately reported the PA-DSS compliance of the Payment Application in accordance with Program requirements, and the detail provided in the ROV meets PCI SSC‘s reporting requirements; 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 procedures.
Delta Assessment	Partial PA-DSS Assessment performed only against applicable PA-DSS Requirements when changes to a listed Payment Application impact only a subset of PA-DSS Requirements.
Dependency	In the context of PA-DSS, a dependency is a specific software or hardware component (such as a database, operating system, API, code library, etc.) necessary for the Payment Application to operate in accordance with the PA-DSS Requirements.
Glossary	Refers to the then-current version of the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*, available on the Website.
Good Standing	a) With respect to a given PA-QSA Company, that the PA-QSA Addendum between the PA-QSA Company and PCI SSC is in full force and effect, the PA-QSA Company has been approved by PCI SSC as a PA-QSA Company and such approval has not been revoked, terminated, suspended, cancelled, or withdrawn, the PA-QSA Company is in compliance with all PA-QSA Requirements, and the PA-QSA Company is not in breach of any of the terms or conditions of remediation, its PA-QSA Addendum (including without limitation, all provisions regarding compliance with the *PA-QSA Qualification Requirements* and payment) or any other agreement with PCI SSC; and b) With respect to a given PA-QSA Employee, that the PA-QSA Employee is in compliance with all PA-QSA Requirements applicable to PA-QSA Employees.

Term	Meaning
List of Validated Payment Applications	Refers to the authoritative list of PA-DSS Validated Payment Applications appearing on the Website.
Listing or listing	Refers to the listing and related information regarding a Payment Application on the List of Validated Payment Applications.
PA-DSS	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Payment Application Data Security Standard and Security Assessment Procedures*, as from time to time amended and made available on the Website.
PA-DSS Assessment	Review of a Payment Application for purposes of validating the compliance of such Payment Application with the PA-DSS as part of the PA-DSS Program.
PA-DSS Program (or Program)	Refers to PCI SSC's program and requirements for qualification of PA-QSA Companies and PA-QSA Employees, and validation and Acceptance of Payment Applications, as further described in this document and related PCI SSC documents, policies and procedures.
PA-DSS Program Guide	The then-current version of (or successor documents to) this document—the *Payment Card Industry (PCI) Data Security Standard (DSS) Payment Application Data Security Standard (PA-DSS) Program Guide*—as from time to time amended and made available on the Website.
PA-DSS Validated Payment Application	A Payment Application that has been assessed and validated by a PA-QSA Company as being compliant with the PA-DSS, then Accepted by PCI SSC, so long as such Acceptance has not been revoked, suspended, withdrawn or terminated.
PA-QSA	Acronym for "Payment Application – Qualified Security Assessor" Company, a company then qualified by PCI SSC to perform PA-DSS Assessments.
PA-QSA Addendum	The then-current version of (or successor document to) the Addendum to Qualified Security Assessor (QSA) Agreement for Payment Application QSAs, the current version of which is attached as Appendix A to the *PA-QSA Qualification Requirements*.
PA-QSA Change Impact	The document template set forth as Appendix D hereto used to describe Administrative, No Impact, and Low Impact changes to a Payment Application; use is mandatory for the PA-QSA Company to submit said changes to PCI SSC, but may also be used by Vendors as a Vendor Change Analysis.
PA-QSA Company	A data security firm that has been qualified, and continues to be qualified, by PCI SSC to perform PA-DSS Assessments for PA-DSS Program purposes.
PA-QSA Company Testing Laboratory (or Laboratory)	A laboratory environment maintained by the PA-QSA Company to perform testing of Payment Applications that Vendors provide for validation.

Term	Meaning
PA-QSA Employee	An individual who is employed by a PA-QSA Company and has satisfied, and continues to satisfy, all QSA and PA-QSA Requirements applicable to employees of PA-QSA Companies who will conduct PA-DSS Assessments, as described in further detail herein.
PA-QSA List	The then-current list of PA-QSA Companies published by PCI SSC on the Website.
PA-QSA Qualification Requirements	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Qualification Requirements for Payment Application Qualified Security Assessors (PA-QSAs)*, as from time to time amended and made available on the Website.
PA-QSA Requirements	With respect to a given PA-QSA Company or PA-QSA Employee, the requirements and obligations thereof pursuant to the *PA-QSA Qualification Requirements*, the PA-QSA Addendum, the PA-DSS Program Guide, each addendum, supplement, and other agreement entered into between such PA-QSA Company or PA-QSA Employee and PCI SSC, and any and all other policies, procedures, requirements, or obligations imposed, mandated, provided for, or otherwise established by PCI SSC from time to time in connection with any PCI SSC program in which such PA-QSA Company or PA-QSA Employee (as applicable) is then a participant, including but not limited to the requirements of all applicable PCI SSC training programs, quality assurance and remediation programs, program guides, and other related PCI SSC program materials.
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 Application	A software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties.
Payment Card Brand	A global payment card brand or scheme that is also a limited liability company member of PCI SSC, currently: American Express, Travel Related Services Company, Inc., DFS Services LLC, JCB Advanced Technologies Inc., MasterCard International Incorporated, Visa International Service Association, and/or their respective affiliates.
PCI SSC	Refers to the PCI Security Standards Council, LLC
ROV	Report containing details documenting results from an entity's PA-DSS Assessment for purposes of the PA-DSS Program.

Term	Meaning
Vendor (or vendor)	A vendor of a Payment Application.
Vendor Change Analysis	Any written description of Administrative, No Impact, or Low Impact changes to a Payment Application prepared by a Vendor and submitted to a PA-QSA Company performing the corresponding PA-DSS Assessment of that Payment Application. The *PA-QSA Change Impact* document template set forth as Appendix D hereto is acceptable for use as a *Vendor Change Analysis* document.
Vendor Release Agreement (or VRA)	The then-current version of (or successor document to) the Payment Card Industry *Vendor Release Agreement* on the form then approved by PCI SSC for Vendors participating in the PA-DSS Program, as from time to time amended and made available on the Website.
Website	The then-current PCI SSC Website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org.
Wildcard	A character that may be substituted for a defined subset of possible characters in an application version scheme. In the context of PA-DSS, wildcards can optionally be used to represent a non-security impacting change. A wildcard is the only variable element of the Vendor's version scheme, and is used to indicate there are only non-security-impacting changes between each version represented by the wildcard element.

1.5 About PCI SSC

PCI SSC reflects a desire among constituents of the Payment Card Industry at all levels for a standardized set of security requirements, security assessment procedures, and processes for recognizing Payment Applications validated by a PA-QSA Company. The PA-DSS and related PCI SSC standards define a common security assessment framework that is recognized by the Payment Card 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 by a PA-QSA Company to meet the PA-DSS Requirements.
- Vendors will only need to have their Payment Applications validated and accepted in accordance with the PA-DSS Program in order for their Payment Applications to be recognized by the participating Payment Card Brands.

For more information regarding PCI SSC, see the Website.

1.6 PA-DSS Alignment Initiative and Overview

This PA-DSS Program Guide reflects a single set of requirements currently recognized by each of the Payment Card Brands regarding:

- Payment Application security requirements and assessment procedures
- Processes for recognizing PA-DSS validated Payment Applications
- Quality assurance processes for PA-QSA Companies

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

Entities that store, process, or transmit cardholder data are required to comply with the PCI DSS. Since Payment Applications are used to store, process, and transmit cardholder data, and entities are required by the Payment Card Brands to be PCI DSS compliant, validated Payment Applications must facilitate—and not prevent—PCI DSS compliance. Examples of how Payment Applications may prevent PCI DSS compliance include:

1. Track data and/or equivalent data on the chip stored in the customer's network after authorization;
2. Applications requiring 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 primary account numbers (PAN), full track data, card validation codes and values (CAV2, CID, CVC2, CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches.

2 Roles and Responsibilities

This section defines requirements that apply for the various roles and responsibilities relating to the management of the Vendor's security policies and procedures. These requirements relate to:

2.1 Vendors

Vendors 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 or negatively impacts 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);
- Educating customers, integrators, and resellers 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 Assessment as specified in *PCI PA-DSS Requirements and Security Assessment Procedures;*
- Complying with the *Vendor Release Agreement* including the adoption and implementation of Vulnerability Handling Policies consistent with industry best practices;
- Creating a *PA-DSS Implementation Guide*, **specific to each application**, in accordance with the requirements in the *PA-DSS;*
- Adhering to their defined software versioning methodology as validated and documented in the ROV;
- Providing their customers via the *PA-DSS Implementation Guide* with any applicable mapping of internally used version numbers to those that have been published (including but not limited to use of wildcards) on the Website; and
- Providing their customers (directly or indirectly through their integrators and resellers) 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 Company for review and authorize their PA-QSA Company to submit resulting ROVs and related information to PCI SSC.

2.2 Payment Card Brands

The Payment Card Brands develop and enforce their own programs related to PA-DSS compliance, including, but not limited to:

- Requirements, mandates, or dates for use of PA-DSS compliant Payment Applications;
- Fines or penalties related to use of non-compliant Payment Applications; and
- Other requirements for using PA-DSS Validated Payment Applications.

2.3 PCI Security Standards Council

PCI SSC is the standards body that maintains the PCI SSC standards, including the PCI DSS, Point-to-Point Encryption (P2PE) standard, PTS, and PA-DSS. In relation to PA-DSS, PCI SSC:

- Maintains a centralized repository for all ROVs;
- Hosts the List of Validated Payment Applications on the Website;
- Provides required training for and qualifies PA-QSA Companies and Employees to assess and validate Payment Applications for PA-DSS compliance;
- Maintains and updates the PA-DSS and related documentation according to a standards lifecycle management process; and
- Reviews all submissions of PA-DSS ROVs and related change submissions for compliance with baseline quality standards, including but not limited to, confirmation that:
  - Submissions (including ROVs, updates and Annual Revalidations) are correct as to form;
  - PA-QSA Companies properly determine whether candidate Payment Applications meet baseline eligibility criteria for validation under the PA-DSS Program (PCI SSC reserves the right to reject or de-list any Payment Application determined to be ineligible for the PA-DSS Program);
  - PA-QSA Companies adequately report the PA-DSS compliance of candidate Payment Applications in their associated submissions; and
  - Detail provided in the Submissions meets PCI SSC's reporting requirements.

As part of the quality assurance (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; assessment and validation is the role of the PA-QSA Company. Listing of a Payment Application on the List of Validated Payment Applications signifies that the applicable PA-QSA Company has determined that the application complies with the PA-DSS, that the PA-QSA Company has submitted a corresponding ROV to PCI SSC, and that the ROV, as submitted to PCI SSC, has satisfied all requirements of the PCI SSC for ROVs as of the time of PCI SSC's review*

2.4 PA-QSA Companies

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

PA-QSA Companies are QSA Companies that are additionally qualified by PCI SSC to perform PA-DSS Assessments. PA-QSA Companies are responsible for:

- Performing PA-DSS Assessments of Payment Applications in accordance with the PA-DSS and the *PA-QSA Qualification Requirements*;
- Providing an opinion regarding whether the Payment Application meets PA-DSS Requirements;
- Documenting each PA-DSS Assessment in a ROV using the PA-DSS ROV Reporting Template;
- Providing adequate documentation within the ROV to demonstrate the Payment Application's PA-DSS compliance;
- Submitting the ROV and/or any change submissions to PCI SSC, along with the *Attestation of Validation* signed by both PA-QSA Company and Vendor;
- Submitting the Payment Application's *PA-DSS Implementation Guide* to PCI SSC;
- Maintaining an internal quality assurance process for their PA-DSS Assessment efforts;
- Staying up to date with Council statements and guidance, industry trends and best practices;

- Properly determining whether or not Payment Applications are eligible for PA-DSS validation; and
- Satisfying all applicable *PA-QSA Qualification Requirements* at all times, including but not limited to successful completion of annual revalidation and all required training and training examinations.

It is the PA-QSA Employee's responsibility to assess a Payment Application's PA-DSS compliance as of the date of the PA-DSS 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.

2.5 Integrators and Resellers

Integrators and Resellers are those entities that sell, install, and/or service Payment Applications on behalf of Vendors or others. Integrators and Resellers 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 Vendor or from the reseller or integrator) with a current copy of the validated Payment Application's *PA-DSS Implementation Guide*.

Integrators and resellers are not permitted to submit Payment Applications to PA-QSA Companies for PA-DSS Assessment. Products can only be submitted by the Vendor.

2.6 Qualified Integrators and Resellers (QIRs)

Note: *Not all integrators and resellers are QIRs—there are additional qualification requirements that must be met for an integrator and reseller to become a QIR.*

PCI Qualified Integrators and Resellers (QIRs) are trained by the Council in PCI DSS and PA-DSS in order to help ensure that they securely implement Payment Applications. For more information on the PCI QIR program, please see www.pcisecuritystandards.org.

2.7 Customers

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

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 Validated Payment Applications to facilitate their PCI DSS compliance are responsible for:

- Ensuring that the Payment Application's version information is consistent with that indicated on the Website;
- Implementing such applications into a PCI DSS compliant environment;
- Configuring such applications (where configuration options are provided) according to the Payment Application's *PA-DSS Implementation Guide* provided by the Vendor;

- Configuring such applications 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 Website along with other reference materials. PCI SSC's List of Validated Payment Applications is the authoritative source for validated Payment Applications that may be used to facilitate a Customer's PCI DSS compliance requirements.

3 Overview of PA-DSS Validation Processes

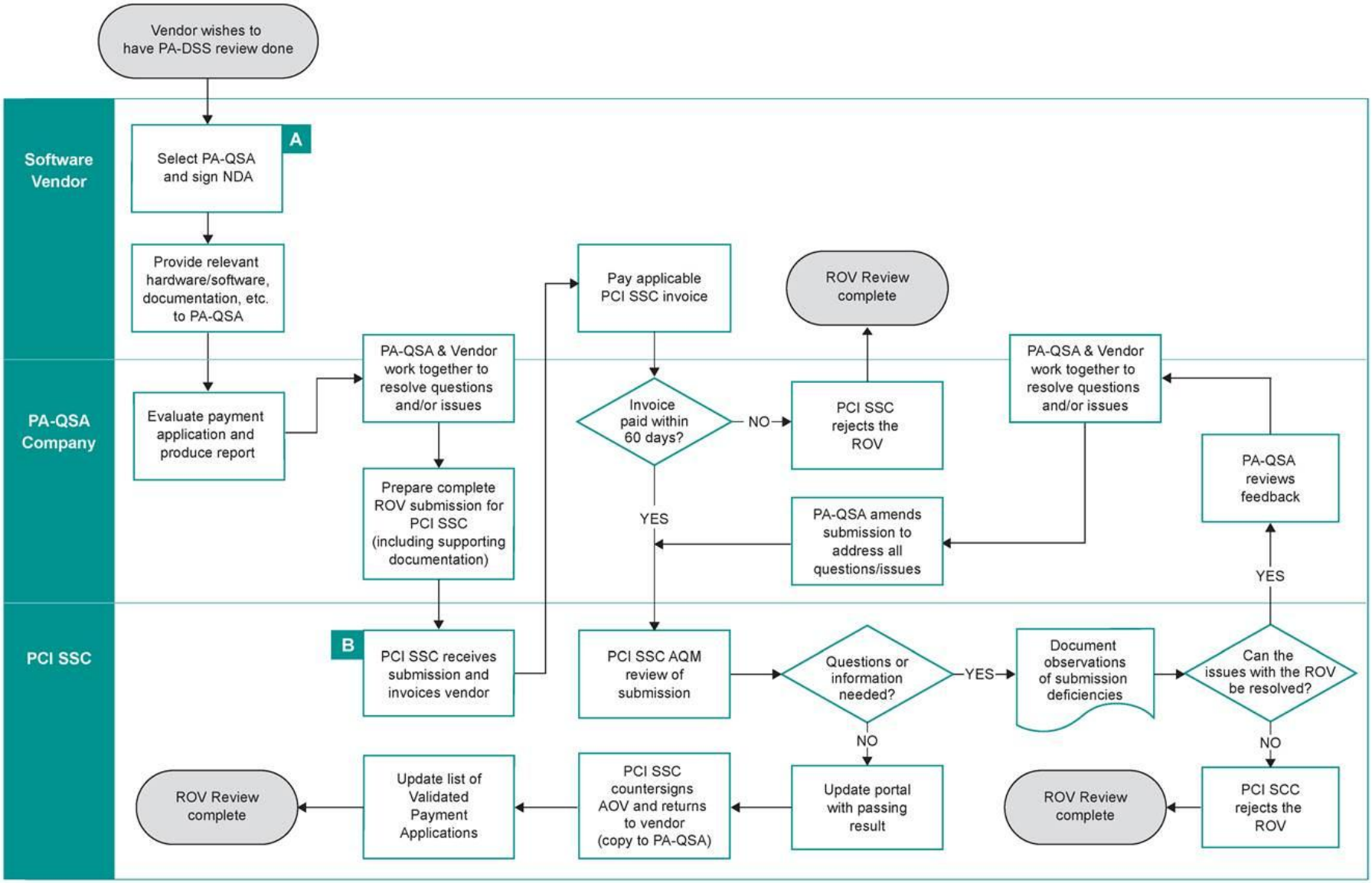
The PA-DSS Assessment process is initiated by the Vendor. The Website has all the associated documents the Vendor will need to navigate the PA-DSS Assessment process. The following is a high-level overview of the process:

1. The Vendor selects a PA-QSA Company from the Council's list of recognized PA-QSA Companies and negotiates the cost and any associated PA-QSA Company confidentiality and non-disclosure agreement with the PA-QSA Company;
2. The Vendor then provides to the PA-QSA Company 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 Company then assesses the Payment Application, including its security functions and features, to determine whether the application complies with the PA-DSS;
4. If the PA-QSA Company determines that the Payment Application is in compliance with the PA-DSS, the PA-QSA Company submits a corresponding ROV to PCI SSC, attesting to compliance and setting forth the results, opinions and conclusions of the PA-QSA Company on all test procedures along with the Vendor's signed VRA and the *Attestation of Validation*;
5. PCI SSC issues an invoice to the Vendor for the applicable PA-DSS Payment Application Acceptance Fee. After the Vendor has paid the invoice, PCI SSC reviews the ROV to confirm that it meets the PA-DSS Program requirements, and if confirmed, PCI SSC notifies the PA-QSA Company and Vendor that the Payment Application has successfully completed the process; and
6. Once the Payment Application successfully completes the above process, the Council signs the *Attestation of Validation* and adds the Payment Application to the List of Validated Payment Applications on the Website.

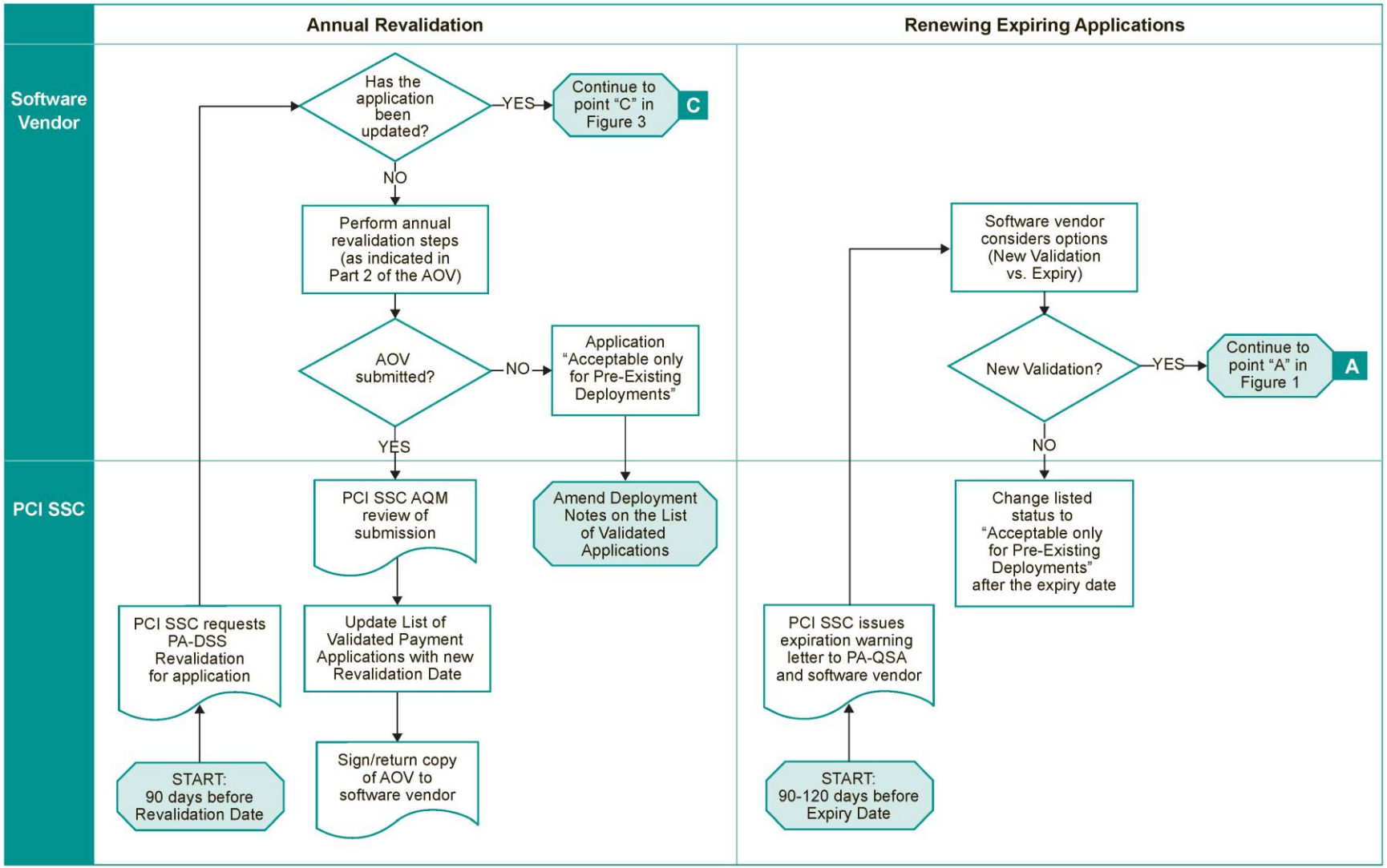
The illustrations and descriptions on the following pages explain in further detail the components of the PA-DSS Program:

Process	Illustration	Page	Related Section
PA-DSS Report on Validation Submittal, Review and Acceptance Process	Figure 1	13	Section 6.1
PA-DSS Annual Revalidation and Renewing Expiring Applications	Figure 2	14	Section 5.4
PA-DSS Updates to Listed Applications	Figure 3	15	Section 5.2

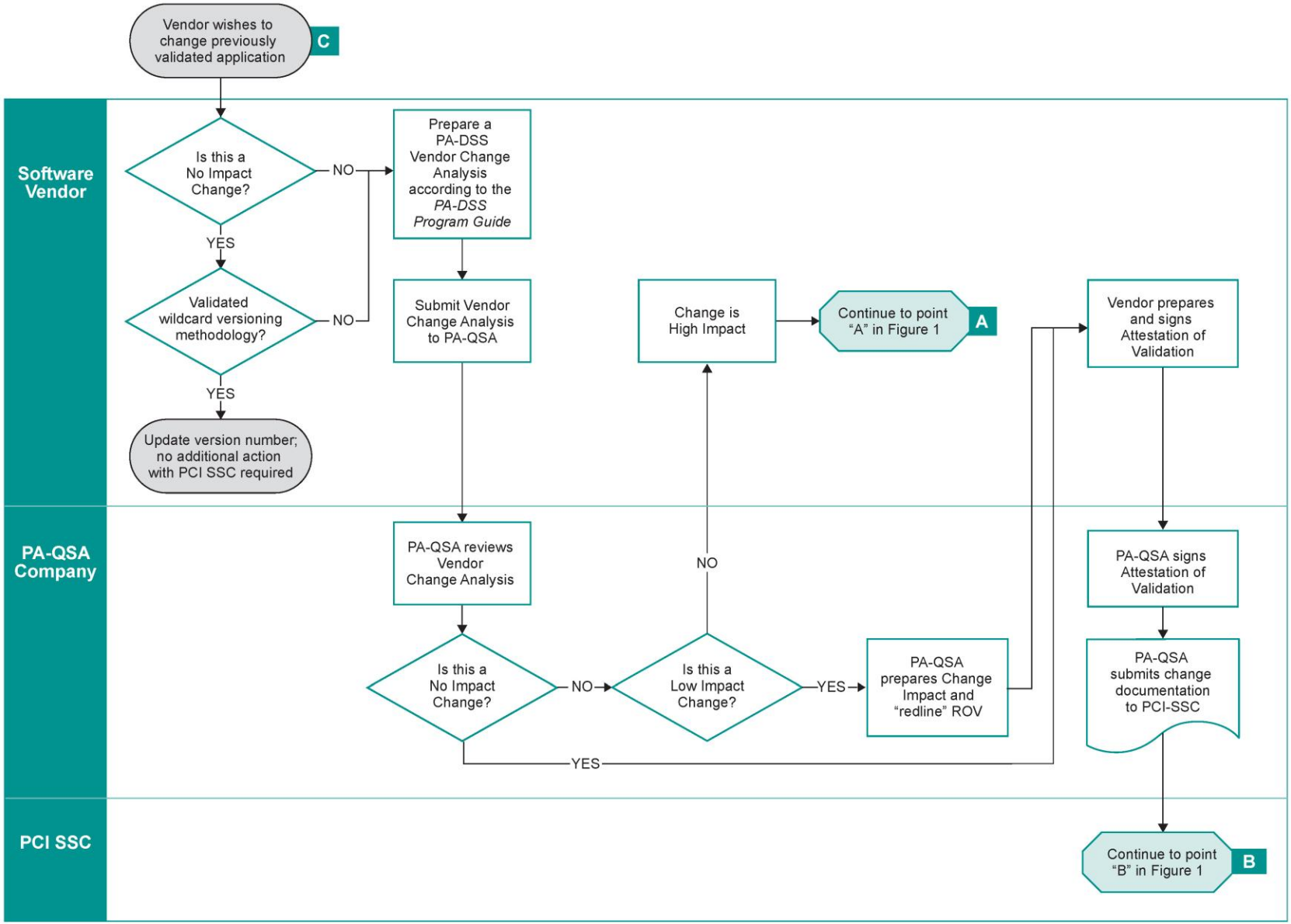
3.1 Figure 1: PA-DSS Report on Validation Submittal, Review and Acceptance Process



3.2 Figure 2: PA-DSS Annual Revalidation and Renewing Expiring Applications



3.3 Figure 3: PA-DSS Updates to Listed Applications



4 Preparation for the Review

4.1 To Which Applications Does PA-DSS Apply?

The following should be used to determine whether PA-DSS applies to a given Payment Application.

- **Table 4.1a** provides a description and program guidance regarding Payment Applications to which PA-DSS **does** apply.
- **Table 4.1b** provides a description and program guidance regarding Payment Applications to which PA-DSS **does not** apply.

Table 4.1a

PA-DSS Applies to:	Program Guidance
Commercial Payment Applications that are typically sold and installed “off the shelf” without pre-installation customization by Vendors.	PA-DSS applies to Payment Applications that do not require re-compilation after merchant- or environment-specific changes. For example, entering or changing parameters such as database names, store locations, etc., during or after installation—but without modification to the executable modules or application code—would not be considered "customizations." However, customer- or environment-specific changes that require modification to the source code and/or re-compilation of the executable (or other payment-processing modules) on a per-merchant basis, prior to installation in the merchant environment, are likely considered to be "customized."
Payment Applications provided in modules, typically including 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 confirmed by a PA-QSA Company as the only one performing payment functions. If other modules also perform payment functions, PA-DSS applies to those modules as well.	It is considered a best practice for 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.

Table 4.1b	
PA-DSS Does Not Apply to:	**Program Guidance**
Payment Applications offered only as a service hosted by a service provider 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 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 such service-type Payment Applications include (but are not limited to): ▪ Those offered by service providers (for example, Application Service Providers, Cloud Service Providers, etc.) who host a Payment Application for their customer's usage. ***Note:*** *PA-DSS would apply if the service provider's Payment Application were also sold to and implemented on a third-party site.* ▪ Virtual payment terminal applications that reside on a service provider's site and are used by merchants to enter their payment transactions. ***Note:*** *PA-DSS would apply if the virtual terminal application has a portion that is distributed to and implemented on the merchant's site.*
Non-Payment Applications that are part of a Payment Application suite, for example, a fraud-monitoring, scoring, or detection application included in a suite.	Such 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.
Payment Applications designed/developed for and sold to a single end-user customer (such as a merchant or service provider) for the sole use of that customer.	Payment Applications developed for and sold to a single customer (such as a merchant or service provider) based on their specifications and for the sole use of that customer, or Payment Applications developed by a merchant or service provider and used only in-house, may be referred to as bespoke Payment Applications. Such Payment Applications would be included as part of the merchant's or service provider's normal PCI DSS compliance efforts and are not eligible for a PA-DSS Assessment.
Payment Applications developed by merchants or service providers used only in-house (not sold, distributed, or licensed to a third party).	

Table 4.1b	
PA-DSS Does Not Apply to:	**Program Guidance**
▪ Operating systems onto which Payment Applications are installed. ▪ Database systems that store cardholder data. ▪ Back-office systems that store cardholder data (for example, for reporting or customer service purposes).	While not intended to be an all-inclusive list, these are examples of platforms and systems which may support Payment Application functions but which are not considered Payment Applications for purposes of PA-DSS, and therefore are not eligible for independent assessment or validation under PA-DSS.

Note: *PCI SSC will only accept and list Payment Applications that are eligible for PA-DSS Assessment, as defined by the PCI SSC.*

4.2 PA-DSS Applicability to Payment Applications on Hardware Terminals

This section provides guidance for Vendors who wish to gain PA-DSS validation for resident Payment Applications on hardware terminals (also known as standalone or dedicated payment 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; or
2. The resident Payment Application does not meet all PA-DSS Requirements, but the hardware on which the application resides 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 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 Assessment, 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 Company must fully test the Payment Application with its dependent hardware against all PA-DSS Requirements. If the PA-QSA Company 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 Company 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 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 Company'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 Payment 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 Vendor and/or the integrator/reseller must package the application for distribution such that it will only operate on the hardware terminal on which it has been validated to run;
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 dependent hardware required for use with the application, in accordance with its PA-DSS validation listing.

4.3 Prior to the Review

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

- Review both PCI DSS and PA-DSS Requirements and related documentation located at the Website;
- Determine/assess the Payment Application's readiness to comply with PA-DSS:
  - Perform a gap analysis between the Payment Application's security functionality and PA-DSS Requirements;
  - Correct any gaps; and
  - If desired, the PA-QSA Company may perform a pre-assessment or gap analysis of a Vendor's Payment Application. If the PA-QSA Company notes deficiencies that would prevent a compliant result, the PA-QSA Company will provide to the 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.

4.4 Required Documentation and Materials

As a requirement for the Assessment, the Vendor must provide the appropriate documentation and software to the PA-QSA Company.

All published PCI SSC information and documents relevant to PA-DSS are available on the 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 Assessment and participation in the PA-DSS Program must be delivered to the PA-QSA Company performing the assessment, not to PCI SSC.

Examples of software, documentation, and other items to submit to the PA-QSA Company include, but are 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. Such documentation includes but is not limited to:
   - *PA-DSS Implementation Guide*;
   - Software Installation Guide or Instructions (as provided to customers);
   - Vendor's software versioning methodology for the application;
   - Vendor's Vulnerability Handling Policies; 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; and
6. The Vendor's executed VRA.

Note: *The PA-QSA Company may request additional material as necessary.*

4.5 PA-DSS Review Timeframes

The amount of time necessary for a PA-DSS Assessment, from the start of an Assessment to listing on the Website can vary widely depending on factors such as:

- How close the application is to being PA-DSS compliant at the start of the Assessment
  - Corrections to the Payment Application to achieve compliance will delay validation.
- Whether the Payment Application's *PA-DSS Implementation Guide* meets all PA-DSS Requirements at the start of the Assessment
  - Extensive rewrites of the *PA-DSS Implementation Guide* will delay validation.
- Prompt payment of the fees due to PCI SSC
  - PCI SSC will not commence review of the ROV until the applicable fee has been paid.
- Quality of the PA-QSA Company's submission to PCI SSC
  - Incomplete submissions or those containing errors—for example, missing or unsigned documents, incomplete or inconsistent submissions—will result in delays in the review process.
  - If PCI SSC reviews the ROV more than once, providing comments back to the PA-QSA Company to address each time, this will increase the length of time for the review process.

Any Assessment timeframes provided by a PA-QSA Company 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 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 (for example, if 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).

4.6 Payment Application Qualified Security Assessors

PCI SSC qualifies and provides required training for PA-QSA Companies and PA-QSA Employees to assess and validate Payment Applications for PA-DSS compliance. In order to perform PA-DSS Assessments, a PA-QSA Company must have been qualified by PCI SSC and remain in good standing as both a QSA Company and PA-QSA Company, and complete all required PA-QSA training. All recognized PA-QSA Companies are listed on the Website. These are the only assessors recognized by PCI SSC as qualified to perform PA-DSS Assessments.

- For each PA-DSS Assessment, the resulting PA-QSA report must follow the PA-DSS Report on Validation (ROV) template and instructions, as outlined in the *PA-DSS ROV Template and PA-DSS ROV Reporting Instructions.*
- The PA-QSA Company must prepare each ROV based on evidence obtained by following the *PA-DSS.*
- Each ROV must be accompanied by an Attestation on Validation (AOV) in the form available through the Website, signed by a duly authorized officer of the PA-QSA Company, that summarizes whether the entity is in compliance or is not in compliance with PCI PA-DSS, and any related findings, as well as the *PA-DSS Implementation Guide.*

4.6.1 Use of the PA-QSA Company Testing Laboratory

PA-QSA Companies are required to test Payment Applications in a pristine computing environment, free from potentially conflicting applications, network traffic, security and/or access controls, software versions, artifacts or "orphaned" components left behind from other software installations. The testing laboratory must be built—and capable of being repeatedly rebuilt—as a predictable, clean merchant environment. The testing laboratory must have the ability to repeatedly return to a known-clean state. If reusing a testing laboratory previously configured for testing a different application or different version of the same application, due diligence must be carried out to ensure that any ghost/orphaned permissions, accounts, registry settings, DLLs, security settings, etc., left over from the previous installation have been removed. Any dependencies, such as operating systems or databases, or PCI DSS-required compliance components, such as firewalls, routers, anti-virus software, intrusion detection/prevention, and file integrity monitoring must restore permissions, accounts, access, stored procedures, etc., to a known, predictable and/or original state.

Note: *Remote access—using two-factor authentication—to the testing laboratory for Payment Application validation is acceptable.*

For each PA-DSS Assessment, PA-QSA testing laboratory processes must include:

- Using the Vendor's installation manual, training provided and the *PA-DSS Implementation Guide* to perform the default installation of the Payment Application.
- Confirming that all implementations of the Payment Application (including region/country specific versions) to be listed were tested in the testing laboratory.

- Confirming that all Payment Application versions and platforms to be listed were tested, including all necessary system components and dependencies.
- Confirming that all critical Payment Application functionalities were tested.
- Confirming that the testing laboratory is capable of simulating the "real world" use of the Payment Application, including:
  - Confirming that the testing laboratory uses only test card numbers.
  - Confirming that the testing laboratory is capable of running authorization and/or settlement functions and that processes include examination of output from all functions.
- Confirming that the testing laboratory is capable of simulating and validating all functions of the Payment Application, which includes that the testing laboratory is capable of exploiting application vulnerabilities.

Use of the PA-QSA Company's Testing Laboratory requires the submission of the Testing Laboratory Configuration for PA-DSS Assessments, found in *ROV Reporting Template* Appendix B, with each PA-DSS Assessment. This form includes a description for the laboratory configuration as part of each PA-DSS Assessment.

In the event that the PA-QSA Company Testing Laboratory is not capable of properly and fully testing all functions of the Payment Application, an alternative laboratory may be used. Testing a Payment Application in an alternative laboratory also requires completion of *ROV Reporting Template,* Appendix B: Testing Laboratory Configuration for PA-DSS Assessments, for each PA-DSS Assessment where an alternative laboratory is used.

4.6.2 PA-QSA Company Fees

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

4.6.3 *Non-PA-DSS assessment* services *that may be offered by PA-QSA Companies*

The list below provides examples of non-PA-DSS Assessment services that may be offered by PA-QSA Companies. These services are neither required nor recommended by PCI SSC. If these services are of interest to your company, please contact the PA-QSA Companies 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 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.

Note: *When arranging for non-PA-DSS Assessment services with a PA-QSA Company, care should be taken by both the Vendor and the PA-QSA Company to ensure that the PA-QSA maintains all independence requirements as set forth in the* QSA Qualification Requirements*, for example, that a PA-QSA Employee does not assess its own work product as part of the actual PA-DSS Assessment. Conflicts of interest may result in a Payment Application's PA-QSA Assessment being rejected by PCI SSC.*

4.7 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 Company.

4.8 Vendor Release Agreement (VRA)

The Vendor's signed copy of the then most current version of the *Vendor Release Agreement* available on the Website must be provided to the PA-QSA Company along with the payment application and other documents and materials at the beginning of each PA-DSS Assessment process, and must be provided to PCI SSC by the PA-QSA Company along with the initial ROV submitted to PCI SSC in connection with that Assessment. Among other things, the VRA covers confidentiality issues, the Vendor's agreement to PA-DSS Program requirements, policies and procedures, and gives permission to the Vendor's PA-QSA Company to release ROVs and related materials to PCI SSC for review. The VRA also requires Vendors to adopt and comply with industry standard Vulnerability Handling Policies. The Vendor's signed copy of the then most current version of the VRA available on the Website must be delivered directly to PCI SSC by the PA-QSA Company, along with the corresponding ROV.

It should be noted that a ROV will not be reviewed by PCI SSC without the then most current VRA on file from the relevant Vendor.

So long as an executed current VRA is on file with the PCI SSC for the relevant Vendor, it is not required to re-submit the same VRA with each subsequent ROV for the same Vendor.

4.9 PA-DSS Payment Application Acceptance Fees

Vendors are also required to pay a *PA-DSS Payment Application Acceptance Fee* to PCI SSC. For each new PA-DSS submission, the *PA-DSS Payment Application Acceptance Fee* will be invoiced, and must be received by PCI SSC before the PA-DSS submission will be reviewed, 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 Company.

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 Website for more information.

PA-DSS Program fees are posted on the Website. Program fees are non-refundable and are subject to change upon posting of revised fees on the Website.

Note:

The Vendor pays all PA-DSS Assessment-related fees directly to the PA-QSA Company (these fees are negotiated between the Vendor and the PA-QSA Company).

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.

5 Managing a Validated Payment Application

5.1 Annual Revalidation

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

As part of this annual process, Vendors are required to confirm whether any changes have been made to the application, and that for all changes that have been made to the application:

a) Changes have been applied in a way that is consistent with the documented software versioning methodology for that application and;

b) The PCI SSC has been advised of any change that necessitates a change to the listing on the Website, in accordance with this Program Guide.

The Vendor is required to consider the impact of external threats, including changes to the environment in which the Payment Application operates. This includes the tested platforms, operating systems and any required dependencies the application may have. For applications included on the "Acceptable for New Deployments" tab on the Website, Vendors are required to confirm that all tested platforms, operating systems, and dependencies upon which the application relies remain supported—for example, that the Vendors (of the operating system, databases, dependent software, etc.) continue to provide patches and updates for any security vulnerabilities identified. If any tested platform, operating system, or dependency is no longer supported at the time of the Annual Revalidation, this must be reflected in the Vendor's response to PCI SSC and will result in an updated listing on the Website to indicate that the Payment Application is "Acceptable only for Pre-Existing Deployments."

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 Payment Applications will be amended to identify that the Payment Application is Acceptable only for Pre-Existing Deployments.

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 the Vendor.

The process flow for annual revalidation is detailed in Figure 2.

5.2 Changes to Listed Payment Applications

Vendors may update listed Payment Applications for various reasons—for example, adding/removing auxiliary functionality, maintaining security updates, or upgrading the baseline or core application. The table below provides a summary of the four types of change scenarios from a PA-DSS perspective:

Change Type	Description
High Impact	Changes to the Payment Application where *any* of the following apply: ▪ Four or more PA-DSS Requirements are affected, not including Requirements 13 and 14; ▪ Half or more of all PA-DSS Requirements/sub-Requirements are affected, not including Requirements 13 and 14; ▪ Half or more of the Payment Application's functionality or half or more of its code-base is changed; ***or*** ▪ Addition of tested platform/operating system to include on the List of Validated Payment Applications. High Impact changes require the Vendor to submit the new version of the Payment Application for a full PA-DSS assessment. *See Section 5.2.3.4, "High Impact Changes," for details.*
Low Impact	Changes to the Payment Application where *all* of the following conditions are met: ▪ Three or fewer PA-DSS Requirements are affected, not including Requirements 13 and 14; ▪ Less than half of all PA-DSS Requirements/sub-Requirements are affected, not including Requirements 13 and 14; and ▪ Less than half the Payment Application's functionality is affected and less than half the Payment Application's code-base is changed. Low Impact changes may be eligible for partial or "delta" assessment. *See Section 5.2.3.3, "Low Impact Changes," for details.*
No Impact	Non-security-related changes that have no impact to PA-DSS related functions, tested platforms, operating systems, or dependencies and no impact on any of the PA-DSS Requirements. No Impact changes may be eligible for partial or "delta" assessment *See Section 5.2.3.2, "No Impact Changes," for details.*
Administrative	Changes to the Payment Application listing or changes to how the Payment Application is described in the List of Validated Payment Applications, for example, corporate identity or application name changes. *See Section 5.2.3.1, "Administrative Changes," for details.*

Note: *While the Payment Application Vendor may choose to continue to support and/or release updates for expired Payment Application versions, PCI SSC does not list changes for expired applications.*

5.2.1 Wildcards

All Payment Application changes must result in a new application version number; however, whether this affects the version number listed on the Website depends on the nature of the change and the Vendor's defined, documented versioning methodology. The use of wildcards may be permitted for managing the versioning methodology for No Impact changes only.

Note: *Wildcards may only be substituted for elements of the version number that represent non-security impacting changes; the use of wildcards for any change that has an impact on security or any PA-DSS Requirements is prohibited.*

Only those applications that have had the Vendor's wildcard versioning methodology assessed to PA-DSS v3.0 by a PA-QSA Company are eligible for wildcard usage, and listing on the PCI SSC website with wildcards. Changes falling within the scope of wildcard usage are not required to be advised to PCI SSC; therefore, any such changes will not result in an update to the application listing on the Website. See Appendix B, Payment Application Software Version Methodology for additional information regarding the use of wildcards.

5.2.2 Delta Assessments

Low Impact and No Impact changes to listed Payment Applications may be eligible for partial re-assessment, or "delta" assessment. It may not be necessary to fully reassess the entire application if a PA-QSA confirms the change has limited impact on the application.

Note: *Only Low Impact and No Impact changes are eligible for delta assessment.*

See "Change Types" section for additional information.

As part of the delta assessment process, the entire Payment Application must be evaluated to determine which PA-DSS Requirements are affected by the change. Delta assessments involve the PA-QSA Company assessing the changes documented in the *Vendor Change Analysis* against the applicable subset of PA-DSS Requirements.

Delta assessments must:

- Be performed by the PA-QSA Company that performed the last Full Assessment and validation of the application;
- Include all PA-DSS Requirements affected by the change;
- Include verification that all other PA-DSS Requirements are *not* affected by the change;

Note: *Due to the likelihood that technical changes to the Payment Application may also impact PA-DSS Requirements 13 and 14, the impact to PA-DSS Requirements 13 and 14 must be considered for every delta assessment.*

- Include details about how, for all PA-DSS Requirements not included in the delta assessment, the PA-QSA verified that those Requirements were *not* affected by the change;
- Include Payment Application functionality testing; and
- Be completed using the same version of the PA-DSS as used for the full validation—for example, a listed Payment Application originally validated against PA-DSS v2.0 cannot have a delta assessment performed using PA-DSS v3.0, and vice-versa.

Delta assessment example

In the example below, a delta assessment may be performed, provided it covers all PA-DSS Requirements impacted by the change and all Payment Application functionality is tested.

Scenario: *A change is made to the mechanism used to securely delete secure authentication data after authorization.*

The Vendor provides the PA-QSA Company with the *Vendor Change Analysis* documentation. The PA-QSA examines the potential impact of the changes, as documented in the *Vendor Change Analysis*, on every PA-DSS Requirement and determines that the change meets the eligibility criteria for a delta assessment after verifying:

- Only PA-DSS Requirements 1, 7, 10, 13 and 14 are affected by the change;
- All other PA-DSS Requirements are *not* affected by the change;
- Less than half the Payment Application's functionality is affected, and less than half of the Payment Application's code-base is changed.

The PA-QSA performs a full assessment of PA-DSS Requirements 1, 7, 10, 13 and 14, performs Payment Application functionality testing, and completes the process in accordance with the Low Impact Changes section of this Program Guide.

5.2.3 Change Types

Since the number of possible Payment Application changes and their impacts cannot be determined in advance, Payment Application changes may be assessed on a per-case basis. Vendors should contact the PA-QSA Company for guidance. Except for No Impact changes covered by the usage of wildcards (as validated during the Payment Application's PA-DSS Assessment), the Vendor prepares documentation of the change (*Vendor Change Analysis*) and submits the *Vendor Change Analysis* to the PA-QSA Company for review. The PA-QSA Company then determines whether a full assessment or delta assessment of the Payment Application is required. This decision is based on the degree to which the changes impact the security and/or PA-DSS related functions of the Payment Application, the impact to PA-DSS Requirements and/or the scope of the changes being made. If the PA-QSA Company is unable to determine the applicable change type, the PA-QSA Company may consult with PCI SSC on an as-needed basis to determine if a change is too great to be eligible for delta assessment.

Note: *The determination of what constitutes a change's type depends on the nature of the change and its impact on the Payment Application or related processes, or PA-DSS Requirements. Working with the Vendor, PA-QSAs have an understanding of the Payment Application and are empowered to determine the change type that represents the proposed change.*

The table on the following page summarizes wildcard usage and delta assessment eligibility for the various change types.

Change Type	Wildcards	Assessment
High Impact	Wildcard usage not permitted	Full PA-DSS Assessment by a PA-QSA required
Low Impact	Wildcard usage not permitted	Eligible for delta assessment by a PA-QSA
No Impact	Wildcard usage permitted[1]	Eligible for delta assessment by a PA-QSA (Delta assessment or Full PA-DSS Assessment are the only options if wildcard versioning was not assessed per PA-DSS v3.0 or above.)
Administrative	N/A	N/A

The following sections provide details about each listed Payment Application change type, the supporting documentation that must be generated and the processes to be followed in order to successfully effect changes to the validation of a listed application.

The process flow for changes to listed Payment Applications is detailed in Figure 3.

5.2.3.1 Administrative Changes

Administrative changes are limited to updates where no Payment Application changes have occurred but the Vendor wishes to request a change to the way the Payment Application is currently listed on the List of PA-DSS Validated Payment Applications on the PCI SSC website. Administrative changes include, but are not limited to, changes to the application name or corporate entity name.

The Vendor prepares a *Vendor Change Analysis* (for example, using the *PA-QSA Change Impact* in Appendix D is acceptable) and submits it to the PA-QSA Company for review.

If the PA-QSA Company agrees with the *Vendor Change Analysis*:

i. The PA-QSA Company must notify the Vendor that they agree;

ii. The Vendor prepares and signs an *Attestation of Validation*, and sends it to the PA-QSA Company;

iii. If applicable, the Vendor modifies the *PA-DSS Implementation Guide* and/or completes a new VRA;

iv. The PA-QSA Company completes the *PA-QSA Change Impact* in Appendix D;

v. The PA-QSA Company signs their concurrence on the *Attestation of Validation* and forwards it, along with the *PA-QSA Change Impact* document to PCI SSC;

vi. PCI SSC will then issue an invoice to the Vendor for the applicable change fee; and

vii. Upon payment of the invoice PCI SSC will review the *Attestation of Validation* and *PA-QSA Change Impact* document for quality assurance purposes.

[1] If a wildcard versioning methodology (as validated during the payment application's PA-DSS Assessment) is used, the No Impact change does not require PA-DSS Assessment, the change is not required to be advised to PCI SSC and the change will not result in any update to the application listing on the PCI SSC website.

If the PA-QSA Company does not agree with the Vendor that the change, as documented in the *Vendor Change Analysis*, has no impact on any functions of the Payment Application, the PA-QSA Company returns the *Vendor Change Analysis* to the Vendor and works with the Vendor to consider the actions necessary to address the PA-QSA Company's observations.

Following successful PCI SSC quality assurance review of the change, PCI SSC will:

i. Amend the List of PA-DSS Validated Payment Applications on the Website accordingly with the new information; and
ii. Sign and return a copy of the *PA-DSS Attestation of Validation* to both the Vendor and the PA-QSA Company. The expiry date of the newly listed application and version number will be the same as that of the parent Payment Application.

For quality issues associated with any aspect of the submission, PCI SSC communicates those issues to the PA-QSA Company, and those issues are resolved according to the process depicted in Figure 1. PCI SSC reserves the right to reject any *Change Impact* document if it determines that a change described therein and purported to be an Administrative Change by the PA-QSA Company or Vendor is ineligible for treatment as an Administrative Change.

5.2.3.2 No Impact Changes

No Impact changes are limited to changes that have no impact to PA-DSS Requirements or Payment Application security, PA-DSS related functions, tested platforms, operating systems or dependencies. Examples of No Impact changes include, but are not limited to user-interface changes, database-schema modifications, updates to reporting modules, and changing/deleting payment gateways.

If the Vendor has chosen to use a wildcard versioning methodology for managing No Impact changes, the wildcard usage must adhere to the requirements in this Program Guide, be consistent with that documented as part of the Vendor's versioning methodology and be validated by the PA-QSA Company as part of the PA-DSS Assessment (PA-DSS v3.0 or above only). Changes falling within the scope of wildcard usage are not required to be advised to PCI SSC, nor will the changes result in any update to the application listing on the PCI SSC website.

If the Vendor has chosen **not** to use a wildcard versioning methodology for managing No Impact changes, the Vendor prepares and submits a *Vendor Change Analysis* (for example, using the *PA-QSA Change Impact* template in Appendix D is acceptable) to the PA-QSA Company that performed the last full validation of the application.

If the PA-QSA Company agrees that the change (as documented by the Vendor in the *Vendor Change Analysis*) meets the No Impact change criteria:

i. The PA-QSA Company must notify the Vendor that they agree;
ii. The Vendor prepares and signs an *Attestation of Validation*, and sends it to the PA-QSA Company;
iii. The PA-QSA Company completes the *PA-QSA Change Impact* template in Appendix D;
iv. The PA-QSA Company signs their concurrence on the *Attestation of Validation* and forwards it, along with the *PA-QSA Change Impact* document and the Payment Application's updated *PA-DSS Implementation Guide,* to PCI SSC;

v. PCI SSC issues an invoice to the Vendor for the applicable change fee; and

vi. Upon payment of the invoice, PCI SSC reviews the *Attestation of Validation* and *PA-QSA Change Impact* document for quality assurance purposes.

If the PA-QSA Company does not agree with the Vendor that the No Impact change (as documented in the *Vendor Change Analysis*) meets the No Impact change criteria, the PA-QSA Company will return the *Vendor Change Analysis* to the Vendor and work with the Vendor to consider the necessary actions to address the PA-QSA Company's observations.

Following successful PCI SSC quality assurance review of the change PCI SSC will:

i. Amend the List of PA-DSS Validated Payment Applications on the Website accordingly with the new information; and

ii. Sign and return a copy of the *PA-DSS Attestation of Validation* to both the Vendor and the PA-QSA Company. The expiry date of the newly listed Payment Application 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 Company, and those issues are resolved according to the process depicted in Figure 1. 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 No Impact change by the PA-QSA Company or Vendor is ineligible for treatment as a No Impact change.

5.2.3.3 Low Impact Changes

PA-QSA Change Impact *document required; may be eligible for delta assessment.*

Low Impact changes are limited to changes to the Payment Application where *all* of the following conditions are met:

- Three or fewer high-level PA-DSS Requirements are affected, not including Requirements 13 and 14;
- Less than half of all PA-DSS Requirements/sub-Requirements are affected, not including Requirements 13 and 14; ***and***
- Less than half the Payment Application's functionality is affected *and* less than half the Payment Application's code-base is changed.

While Low Impact changes are not eligible for wildcard versioning, they are eligible for delta assessment. Examples of Low Impact changes to PA-DSS related functions of a Validated Payment Application include, but are not limited to:

- Inclusion of updates or patches to validated OS versions upon which the Payment Application was previously validated;
- Inclusion of updates or patches to supported third-party databases with which the Payment Application was previously validated;
- Additions or deletions of supported payment processors;
- Inclusion of updates or patches to supported middleware with which the Payment Application was previously validated;
- Recompilation of unchanged code base with either the same compiler using different flags or with a completely different compiler;

Note: *It is strongly recommended that the Vendor uses the PA-QSA Company that performed the last full Payment Application assessment, as changing PA-QSA Companies requires a full assessment.*

- Changes to the software versioning methodology for the Payment Application;
- Inclusion of non-security related patches to the Payment Application.

Since the number of possible Payment Application changes and their impacts cannot be determined in advance, the type of assessment performed for Low Impact changes may be considered on a per-case basis. Vendors should contact the PA-QSA Company that performed the last full validation of the Payment Application for guidance. The PA-QSA Company determines whether a full assessment or delta assessment of the Payment Application is required, based on the degree to which the changes impact the security and/or PA-DSS related functions of the Payment Application, the impact to PA-DSS Requirements and/or the scope of the changes being made.

The Vendor prepares and submits a *Vendor Change Analysis* (for example, using the *PA-QSA Change Impact* document in Appendix D is acceptable) to the PA-QSA Company that performed the last Full validation of the application.

If the PA-QSA Company agrees that the change (as documented by the Vendor in the *Vendor Change Analysis*) meets the Low Impact change criteria and is eligible for a delta assessment:

i. The PA-QSA Company must notify the Vendor that they agree;
ii. The PA-QSA Company performs a delta review of the Payment Application for the PA-DSS Requirements affected by the Low Impact change;
iii. The PA-QSA Company tests the Payment Application's functionality;
iv. The PA-QSA Company completes a *PA-QSA Change Impact* document in Appendix D and makes redline changes to the original ROV as appropriate;
v. The Vendor prepares and signs an *Attestation of Validation* and sends it to the PA-QSA Company;
vi. The PA-QSA Company 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;
vii. PCI SSC issues an invoice to the Vendor for the applicable change fee; and
viii. Upon payment of the invoice, PCI SSC will review the *Attestation of Validation,* the "redline" version of the ROV and the *PA-QSA Change Impact* document for quality assurance purposes.

If the revision is deemed by the PA-QSA Company to be ineligible for delta assessment, the PA-QSA returns the *Vendor Change Analysis* to the Vendor and works with the Vendor to consider what actions are necessary to address the PA-QSA Company's observations.

Following successful PCI SSC quality assurance review of the change, PCI SSC will:

i. Amend the *List of PA-DSS Validated Payment Applications* on the Website accordingly with the new information; and
ii. Sign and return a copy of the *Attestation of Validation* to both the Vendor and the PA-QSA Company. The expiry date of this newly listed application will be the same as that of the parent Payment Application.

For quality issues associated with any aspect of the submission, PCI SSC communicates those issues to the PA-QSA Company, and those issues are resolved according to the process depicted in Figure 1. 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 Company or Vendor is ineligible for treatment as a Low Impact change.

5.2.3.4 High Impact Changes

Full PA-DSS Assessment is required.

If changes to the Payment Application meet **any** of the following criteria, the Payment Application must undergo a full PA-DSS Assessment:

- Four or more high-level PA-DSS Requirements are affected, not including Requirements 13 and 14;
- Half or more of all PA-DSS Requirements/sub-Requirements are affected, not including Requirements 13 and 14;
- Half or more of the Payment Application's functionality is affected, or half or more of the Payment Application's code-base is changed;
- Addition of tested platform/operating system to include on the List of Validated Payment Applications; ***or***
- The change is otherwise ineligible for treatment as a Low Impact change.

The PA-QSA Company 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 Company, who will determine whether the nature of the change impacts Payment Application security in accordance with current PA-DSS Requirements.

5.3 Change Documentation

Administrative Change	No Impact Change [2]	Low Impact Change	High Impact Change or New Application
▪ *Attestation Of Validation* ▪ *PA-QSA Change Impact* document ▪ *PA-DSS Implementation Guide* * ▪ *Vendor Release Agreement* (one per Vendor) * ▪ Fee	▪ *Attestation Of Validation* ▪ *PA-QSA Change Impact* document ▪ *PA-DSS Implementation Guide* ▪ Fee	▪ *Attestation Of Validation* ▪ *PA-QSA Change Impact* document ▪ Report On Validation Redline ▪ *PA-DSS Implementation Guide* ▪ Fee	▪ *Attestation Of Validation* ▪ Report On Validation ▪ *PA-DSS Implementation Guide* ▪ *Vendor Release Agreement* (one per Vendor) * ▪ Fee

** If applicable*

Note: *The* PA-QSA Change Impact *document in Appendix D is mandatory for the PA-QSA Company for submitting Administrative, No Impact and Low Impact changes to PCI SSC but may also be used by Vendors as a* Vendor Change Analysis.

[2] If a wildcard versioning methodology (as validated during the payment application's PA-DSS Assessment) is used, the No Impact change does not require PA-DSS Assessment, the change is not required to be advised to PCI SSC, and the change will not result in any update to the application listing on the PCI SSC website.

5.4 Renewing Expiring 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 either new validation or expiry:

1. **New Validation**: If the Vendor wishes the application to remain on the *Acceptable for New Deployments List* on the Website, the Vendor must contact a PA-QSA Company to have the Payment Application fully re-evaluated against the then-current version of the PA-DSS. Use of the Low/No Impact or Administrative Change process to achieve this goal is not permitted.
2. **Expiry:** In all other situations where the Vendor fails to submit the application for full re-assessment by the expiry date, PCI SSC will change the listed status of the Payment Application to "Only Acceptable for **Pre**-Existing Deployments" after the expiry date.

Note that if the expiring application successfully completes the PA-DSS Assessment process again, the re-validated application retains its status on the List of Validated Payment Applications as Acceptable for New Deployments and is assigned a new expiry date.

The process flow for renewing expiring applications is detailed in Figure 2.

5.5 Validation Maintenance Fees

If a listed Payment Application is revised, the Vendor is required to pay the applicable change fee to PCI SSC.

For any change affecting the listing of a validated Payment Application, the applicable fee will be invoiced and must be received by PCI SSC for the changes to be Accepted and added to the *PCI SSC* List of Validated Payment Applications. Upon Acceptance, PCI SSC will sign and return a copy of the *Attestation of Validation* to both the Vendor and the PA-QSA Company.

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

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

Note:

The *Vendor pays all PA-DSS Assessment-related fees directly to the PA-QSA (these fees are negotiated between the Vendor and the PA-QSA Company).*

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.

5.6 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").

5.6.1 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.

Note: *Notification must take place no later than 24 hours after the Vendor first becomes aware of the Security Issue.*

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

5.6.2 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 PA-DSS Program Manager at (781) 876-8855.

5.6.3 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 the information required by the *Vendor Release Agreement*. At a minimum, this must include:

- The name, PCI SSC reference number, and any other relevant identifiers of the Payment Application;
- A description of the general nature of the Security Issue;
- The Vendor's good-faith assessment, to its knowledge at the time, as to the scope and severity of the vulnerability or vulnerabilities associated with the Security Issue (using CVSS or other industry accepted standard scoring);
- Assurance that the Vendor is following their Incident Response and/or Vulnerability Handling Policies.

5.6.4 Actions following a Security Breach or Compromise

In the event of PCI SSC being made aware of a Security Issue related to a PA-DSS Validated Payment Application, PCI SSC may take the actions specified in the VRA and additionally, may:

- Notify participating Payment Card Brands that a Security Issue has occurred.
- Request a copy of the latest version of the Vendor's Vulnerability Handling Policies.
- Communicate with the Vendor about the Security Issue and, where possible, share information relating to the Security Issue.
- Support the Vendor's efforts to mitigate or prevent further Security Issues.
- Support the Vendor's efforts to correct any Security Issues.
- Work with the Vendor to communicate and cooperate with appropriate law enforcement agencies to help mitigate or prevent further Security Issues.

5.6.5 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 VRA, in instances including, but not limited to, if PCI SSC reasonably determines that (a) the Payment Application does not offer sufficient protection against current threats and does not conform to PA-DSS Requirements, or (b) the continued Acceptance of the Payment Application represents a significant and imminent security threat to its users, or (c) the Payment Application is subject to a Security Issue.

6 PA-DSS Assessment Reporting Considerations

6.1 PA-DSS Report Acceptance Process Overview

The PA-QSA Company performs the PA-DSS Assessment in accordance with the *PA-DSS Requirements and Security Assessment Procedures*, and produces a ROV that is shared with the Vendor. When the ROV has all items in place, the PA-QSA Company submits the ROV and all other required materials to PCI SSC. If the ROV does not have all items in place, the Vendor must address those items, and the PA-QSA Company must update the ROV prior to submission to PCI SSC. For example, this may include updating user documentation or software. Once the PA-QSA Company is satisfied that all documented issues have been resolved by the Vendor, the PA-QSA Company submits the ROV and all other required materials to PCI SSC.

Note:

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

Once PCI SSC receives the ROV and all other required materials and applicable fees, PCI SSC reviews the ROV from a quality assurance perspective. If the ROV meets all applicable quality assurance requirements (as documented in the *QSA Qualification Requirements* and related program materials), PCI SSC sends a countersigned PA-DSS *Attestation of Validation* to both the Vendor and the PA-QSA Company, and adds the application to the List of Validated Payment Applications.

PCI SSC communicates any quality issues associated with ROVs to the PA-QSA Company. It is the responsibility of the PA-QSA Company to resolve the issues with PCI SSC and/or the Vendor, as applicable. Such issues may be limited or more extensive; limited issues may simply require updating the ROV to reflect adequate documentation to support the PA-QSA Company's decisions, whereas more extensive issues may require the PA-QSA Company to perform further testing, requiring the PA-QSA Company to notify the Vendor that re-testing is needed and to schedule that testing with the Vendor.

ROVs that have been returned to the PA-QSA Company for correction must be resubmitted to the PCI SSC within 30 days of the preceding submittal. If this is not possible, the PA-QSA Company must inform the PCI SSC of the timeline for response. Lack of response on ROVs returned to the PA-QSA Company 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 submissions.

The process flows for ROV Acceptance and ROV Review Process are detailed in Figure 1.

6.2 Delivery of the ROV and Related Materials

All documents required in connection with the PA-DSS validation process must be submitted to PCI SSC by the PA-QSA Company, through a secure submissions website designated by PCI SSC (the Portal). Council staff pre-screen Portal submissions to ensure that all required documentation has been included and the basic submission requirements have been satisfied.

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, incomplete or inconsistent documentation, application dependencies being insufficiently explained, and tested platforms/operating systems being insufficiently explained. 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.

6.2.1 Access to the Portal

Once a PA-QSA Company has had its first employee successfully 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 Contact. Additional credentials can be requested by each company's Primary PA-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-QSA Employees.

6.2.2 Listing Information

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

***Note**:*
All descriptions must be acceptable to PCI SSC, which reserves the right to modify any description at any time.

6.3 Assessor Quality Management Program

As stated in the *QSA Qualification Requirements* and the PA-QSA Addendum, PA-QSA Companies are required to meet all quality assurance standards set by PCI SSC. The various phases of the assessor quality management program are described below.

The process flow for the QA program is detailed in Figure 4.

6.3.1 ROV Submission Reviews

PCI SSC's Assessor Quality Management Team ("AQM") reviews each ROV submission after the invoice has been paid by the Vendor. Administrative review will be performed in "pre-screening" to ensure that the submission is complete, then an AQM analyst will review the submission in its entirety.

The AQM analyst will review the application first to determine whether it is eligible for validation as described in the *PA-DSS Program Guide*. If there is question as to eligibility, the AQM analyst will contact the PA-QSA Company for additional information. If the Payment Application is determined to be ineligible for validation under the PA-DSS Program, the ROV will be rejected. The PA-QSA Company will receive a letter of rejection with optional instructions for appealing the rejection.

If the Payment Application is determined to be eligible for validation under the PA-DSS Program and the submission is complete, the AQM analyst will complete a full review of the ROV submission and the supporting documentation provided or requested subsequently. Any comments or feedback from the AQM analyst will be made via the Portal, and the PA-QSA Company is expected to address all comments and feedback in a timely manner. The AQM analyst's role is to ensure sufficient evidence and detail is present in the PA-QSA Company's submission to provide reasonable assurance of a quality assessment.

6.3.2 PA-QSA Quality Audit

The purpose of the PA-QSA Company audit process is to provide reasonable assurance that the assessment of Payment Applications and overall quality of report submissions remain at a level that is consistent with the objectives of the *PA-DSS Program Guide* and supporting PCI SSC documentation.

QSA Company audits are addressed in the *QSA Qualification Requirements*, and PA-QSA Companies may be subject to audits of their work under the *QSA Qualification Requirements* at any time. This may include, but not be limited to, review of completed reports, work papers and onsite visits with PA-QSA Companies to audit internal QA programs, at the expense of the PA-QSA Companies. Refer to the *QSA Qualification Requirements* for information on PCI SSC's audit process.

6.3.3 PA-QSA Company Status

The PA-DSS Program recognizes several status designations for PA-QSA Companies: "In Good Standing," "Remediation," and "Revocation." The status of a PA-QSA Company is typically "In Good Standing" but may change based on quality concerns, feedback from clients and/or Payment Card Brands, administrative issues, or other factors. These status designations are described further below.

Note: *These status designations are not necessarily progressive: Any PA-QSA Company's status may be revoked or its PA-QSA Addendum terminated in accordance with the PA-QSA Addendum; and accordingly, if warranted, a PA-QSA Company may move directly from "In Good Standing" to "Revocation."*

Nonetheless, in the absence of severe quality concerns, PA-QSA Companies with quality issues are generally first addressed through the Remediation process in order to promote improved performance.

6.3.3.1 In Good Standing

PA-QSA Companies are expected to maintain a status of In Good Standing while participating in the PA-DSS Program. Reviews of each submission and the overall quality of submissions will be monitored by PCI SSC to detect any deterioration of quality levels over time. The PA-QSA Company may also be subject to periodic audit by PCI SSC at any time.

6.3.3.2 Remediation

A PA-QSA Company and/or PA-QSA Employee may be placed into Remediation for various reasons, including administrative issues or quality concerns. PA-QSA Companies and/or Employees in Remediation are listed on the Website in red, indicating their remediation status without further explanation as to why the designation is warranted.

If non-severe quality problems are detected, PCI SSC will typically recommend participation in the Remediation program. While participation is optional, Remediation provides an opportunity for PA-QSA Companies and/or Employees to improve performance by working closely with PCI SSC staff; and in the absence of participation, quality issues may increase. Additionally, Remediation helps to assure that the baseline standard of quality for PA-QSA Companies and/or Employees is upheld. Refer to the *QSA Qualification Requirements* for further detail on the Remediation Process.

Note:

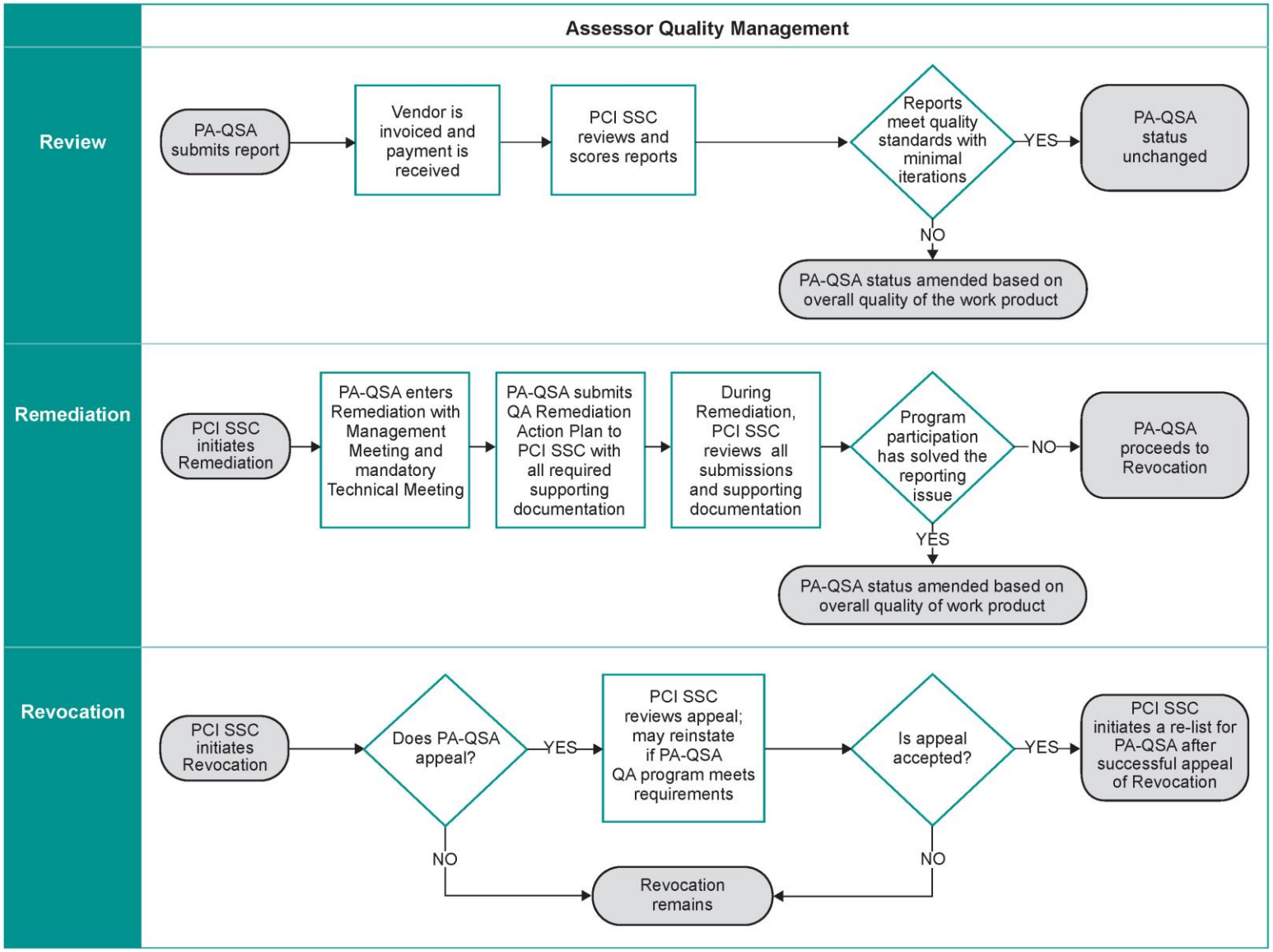
If a Payment Application included on the PCI SSC List of PA-DSS Validated Payment Applications is compromised due to PA-QSA Company and/or Employee error, that PA-QSA Company and/or Employee may immediately be placed into Remediation or its status revoked.

6.3.3.3 Revocation

Serious quality problems may result in revocation of PA-QSA Company and/or PA-QSA Employee qualification and termination of the PA-QSA Addendum. When a PA-QSA Company's and/or Employee qualification is revoked, the assessor is removed from the PA-QSA List and is no longer eligible to perform PA-DSS 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 Company and/or Employee 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 Company and/or Employee may appeal the Revocation, but unless otherwise approved by PCI SSC in writing in each instance, will not be permitted to perform PA-DSS Assessments, process ROVs, or otherwise participate in the PA-DSS Program. The PA-QSA Company and/or Employee may reapply at a later date of one year after revocation, so long as it has demonstrated to PCI SSC's satisfaction that it meets all applicable QSA and PA-QSA Requirements as documented in the *QSA Qualification Requirements*, *PA-QSA Qualification Requirements* and relevant PCI SSC program documents.

6.4 Figure 4: PA-QSA QA Programs for Report Reviews



Note: *"PA-QSA" refers to PA-QSA Company and/or PA-QSA Employee*

7 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 (or eligible wildcard) of that Payment Application that was reviewed by a PA-QSA Company and subsequently accepted by PCI SSC (the Accepted Version). If any aspect of a Payment Application or version thereof is different from the Accepted Version—even if the different Payment Application or version (the Alternate Version) conforms to the basic product description of the Accepted Version—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 Accepted," 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 actually issued an *Attestation of Validation* with respect to the Approved Version of a Payment Application, such Approved Version may be referred to as PCI SSC Accepted or listed. 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 Company has determined that the Accepted Version of 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 AQM review, but such Acceptance does not under any circumstances include or imply any endorsement or warranty by PCI SSC or any Payment Card 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, if at all, by the party providing such products or services, and not by PCI SSC or any Payment Card 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.x
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. The Payment Application Name cannot contain any variable characters.

  The PCI SSC's various Program names and/or acronyms (e.g., PCI DSS, PA-DSS, PTS, etc.) are strictly prohibited from use in Vendor Payment Application Names. PCI SSC reserves the right to reject any Payment Application of which any such Program name or acronym is a part.

- **Payment Application Version #**

  Payment Application Version # represents the application version reviewed in the PA-DSS Assessment. The format of the version number:

  - Is set by the Vendor;
  - May consist of alphanumeric characters and;
  - Must be consistent with the Vendor's published versioning methodology for this product as documented in the *PA-DSS Implementation Guide*.

Note:
See Appendix B: Payment Application Software Version Methodology for details about content to include in the ROV and PA-DSS Implementation Guide *for Vendor's versioning methods*.
Customers are strongly advised to deploy only those Payment Applications with the Application Version # whose characters are consistent with the Application Version # shown on the List of Validated Payment Applications.

- **Payment Application Type**

  Payment Applications can have many functions. The Vendor must choose the option which best describes the primary function of the application from the list below.

Type	Function	Description
01	POS Suite/General	Point of sale software that 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 that 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, then 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.

Type	Function	Description
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.
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 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 change reference	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 Applications, should the ROV be accepted. This must be a factual description of the application functionality and, optionally, the target market. The description must not:

- Contradict any PCI SSC program or requirement (e.g., the application must not claim to store sensitive authentication data after authorization).
- Make misleading claims about the application (e.g., that usage of the application reduces the scope of a PCI DSS Assessment).
- Claim the application is valid under another PCI SSC program or standard.

PCI SSC recommends keeping the description concise and including only pertinent information about the application.

All descriptions must be acceptable to PCI SSC, which reserves the right to modify any description at any time.

A.4 Tested Platforms/Operating Systems

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

Only the specific operating systems and platforms on which the application was tested will be listed on the Website.

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 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 revalidation, 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 Deployments**: All newly Accepted PA-DSS Validated Payment Applications are initially put into this state and will maintain this state until such time that either (i) annual revalidation requirements are not maintained by the Vendor causing an early administrative 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.
- **Acceptable only 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 early administrative 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. Questions about continued use of validated Payment Applications that have expired should be referred to the Payment Card Brands.

These deployment notes are used by the Council to note the status of a Validated Payment Application in relation to its Expiry Date. See table under "Expiry Date" below for examples.

Please refer to specific Payment Card Brand requirements for usage of Validated Payment Applications.

A.8 Revalidation Date

The **Revalidation Date** is used by PCI SSC to indicate when the 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 have 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 3.0 will have an expiration date of 2019 as the next PA-DSS version is expected to be released in October 2016; while reviews against PA-DSS Versions 2.0 will expire in October 2016.

Payment Card Brands have their own compliance programs for the usage of PA-DSS Validated Payment Applications. Questions on how using an application listed as Acceptable only for Pre-Existing Deployments affects PCI DSS compliance must be addressed to the merchant's acquirer and/or the Payment Card Brands involved.

Validation Notes	Expiry Date	Deployment Notes	Annual Revalidation Required
Validated According to PA-DSS (PA-DSS v3.0)	28 October 2019	Acceptable for New Deployments	Yes
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 only for Pre-Existing Deployments	No
Validated According to PABP (PABP 1.4)	2 March 2011	Acceptable only for Pre-Existing Deployments	No
Validated According to PABP (PABP 1.3)	2 June 2010	Acceptable only for Pre-Existing Deployments	No
Pre-PCI SSC Application (Prior to PABP 1.3)	2 December 2009	Acceptable only for Pre-Existing Deployments	No

A.10 PA-QSA Company

This entry denotes the name of the PA-QSA Company that performed the validation and determined that the Payment Application is compliant with PA-DSS.

Appendix B: Payment Application Software Versioning Methodology

Vendors are required to document and follow a software versioning methodology as part of their system development lifecycle. Additionally, Vendors must communicate the versioning methodology to their customers and integrators/resellers in the *PA-DSS Implementation Guide*. Customers and integrators/resellers require this information to understand which version of the application they are using and, the types of changes that have been made to each version of the application. PA-QSA Companies are required to verify the Vendor is adhering to the documented versioning methodology and the requirements of the *PA-DSS Program Guide* as part of the PA-DSS Assessment. Note that if a separate version-numbering scheme is maintained internally by the Vendor, a method to accurately map the internal version numbers to the publically listed version number(s) must be documented and maintained by the Vendor.

B.1 Version Number Format

The format of the application version number is set by the Vendor and may be comprised of several elements. The versioning methodology and the *PA-DSS Implementation Guide* must fully describe the format of the application version number including the following:

- The format of the version scheme, including:
  - Number of elements
  - Numbers of digits used for each element
  - Format of separators used between elements
  - Character set used for each element (consisting of alphabetic, numeric, and/or alphanumeric characters)
- The hierarchy of the elements
  - Definition of what each element represents in the version scheme
  - Type of change: major, minor, maintenance release, wildcard, etc.
- The definition of elements that indicate any use of wildcards
- The specific details of how wildcards are used in the versioning methodology

B.2 Version Number Usage

All changes to the Payment Application must result in a new application version number. However, whether this affects the version number listed on the Website depends on the nature of the change and the Vendor's published versioning methodology (see Section B.3 "Wildcards" below). All changes that impact security functionality and/or any PA-DSS Requirements must result in a change to the version number listed on the Website; wildcards are not permitted for changes impacting security functionality and/or any PA-DSS Requirements.

The Vendor must document how elements of the application version number are used to identify:

- Types of changes made to the application—e.g., major release, minor release, maintenance release, wildcard, etc.
- Changes that have no impact on the functionality of the application or its dependencies
- Changes that have impact on the application functionality but no impact on security or PA-DSS Requirements
- Changes that impact any security functionality or PA-DSS Requirement

Elements of the version number used for non-security-impacting changes must never be used for security-impacting changes.

If the Vendor uses a versioning scheme that involves mapping of internal version numbers to external, published version numbers, all security-impacting changes must result in an update to the external, published version number.

Any version number that is accessible to customers and integrator/resellers must be consistent with the versioning methodology described in the *PA-DSS Implementation Guide*.

Vendors must ensure traceability between application changes and version numbers such that a customer or integrator/reseller may determine which changes are included in the specific version of the application they are running.

B.3 Wildcards

A "wildcard" element is a variable character that may be substituted for a defined subset of possible characters in an application versioning scheme. In the context of PA-DSS, wildcards can optionally be used to represent non-security-impacting changes between each version represented by the wildcard element. A wildcard is the only variable element of the Vendor's version scheme. Use of a wildcard element in the versioning scheme is optional and is not required in order for the Payment Application to be PA-DSS validated. The use of wildcard elements is permitted subject to the following:

a. Wildcard elements may only be used for No Impact changes, which have no impact on security and/or any PA-DSS Requirements.

b. The use of wildcard elements is limited to the rightmost (least significant) portion of the version number. For example, *1.1.x* represents acceptable usage. A version methodology that includes a wildcard element followed by a non-wildcard element is not permitted. For example, *1.x.1* and *1.1.y.1* represent usage that is not permitted.

c. All security-impacting changes must result in a change to the non-wildcard portion of the application version number and will therefore result in an update to the version number listed on the Website.

d. Wildcard elements must not precede version elements that could represent security-impacting changes.

e. All wildcard usage must be pre-defined and documented in the Vendor's versioning methodology and the *PA-DSS Implementation Guide*.

f. All wildcard usage must be consistent with that validated by the PA-QSA Company as part of the PA-DSS Assessment of the Payment Application.

Appendix C: Identification of Certified Payment Application Builds

Note: *For future consideration*

While certified Payment Application builds are not a requirement at this time, we encourage Vendors and PA-QSA Companies 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 Company as PA-DSS compliant should be fingerprinted—digitally signed (code-signed)—by both the 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 Payment Card Brand related PA-DSS programs and help foster customer awareness and confidence.

Appendix D: PA-QSA Change Impact

Administrative, No Impact (if a validated wildcard versioning methodology is not used), and Low Impact changes to PA-DSS Validated Payment Applications must be disclosed in this *PA-QSA Change Impact* document. Note that all High Impact changes require a full PA-DSS Assessment.

PA-QSA must complete each section of this document, and all required documents based on the type of change (see "Required Documents" section below). The PA-QSA is required to submit this *PA-QSA Change Impact* along with supporting documentation to PCI SSC for review.

Always refer to the applicable *PA-DSS Program Guide* for information on Payment Application changes.

Payment Application Details			
Name of Payment Application		Application Version	
Validation PA-DSS Standard		Validated Listing Reference #	
Submission Date			
Type of Change (please check)	☐ Administrative	☐ No Impact	☐ Low Impact

Payment Application Vendor Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	
PA-QSA Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	
PA-QSA QA Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	

Change Revision			
Revised Company Name (if applicable)			
Revised Application Name (if applicable)		Revised Application Version	
Description of how this change is reflected in the Vendor's versioning methodology, including how this version number indicates the type of change			

Required Documents (indicated with an "x")						
Type of Change	**PA-DSS Implementation Guide**	**Attestation of Validation (AOV)**	**PA-QSA Change Impact**	**Red-lined ROV**	**Report on Validation (ROV)**	**Vendor Release Agreement (VRA)**
Administrative Change	*	X	X			*
No Impact Change (with no wildcard versioning)	X	X	X			
Low Impact Change	X	X	X	X		
High Impact Change	X	X			X	*

** If applicable*

Change Impact Details

For **each** change, provide the following information. Any that impact PA-DSS Requirements must be reflected in the Redline ROV submitted. Use additional pages if needed.

Indicate which PA-DSS Requirements are impacted by the change:													
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6	☐ 7	☐ 8	☐ 9	☐ 10	☐ 11	☐ 12	☐ 13	☐ 14

Note: *At a minimum, PA-DSS Requirements 13 & 14 must be assessed.*

If any PA-DSS Requirements were excluded from the assessment, provide a description of the testing performed to validate that excluded PA-DSS Requirements ***are not*** impacted (for example, comparing code, *Vendor Change Analysis,* details from developer interviews, details from functionality testing, etc.):

Change Number	Detailed description of the change	Description of why the change is necessary	Description of how CHD is impacted	Description of how the change impacts application functionality