Payment Card Industry (PCI)

Payment Application Data Security Standard (PA-DSS)

Program Guide

Version 2.1

March 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.
March 2014	2.1	• To implement minor process and terminology changes noted since *PA-DSS Program Guide* v2.0. • Addition of "Qualified Integrators and Resellers" section to explain how the new QIR Program aligns with the PA-DSS Program. • Minor change to the process for submitting a ROV to allow PCI SSC to invoice the Vendor upon receipt of a ROV and receive payment prior to reviewing the ROV. • Change "Quality Assurance Program" section to "Assessor Quality Management Program" and update processes accordingly. • Clarify Vendor requirements in Appendix A for Payment Application description.

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, the PCI SSC has adopted and maintains the Payment Card Industry 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 compliance is important to the effectiveness of the Program.

To help merchants and service providers achieve this goal, PCI SSC manages the PA-DSS 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:

- *Payment Card Industry (PCI) Payment Application Data Security Standard – Requirements and Security Assessment Procedures v2.0* ("PA-DSS")
- *Payment Card Industry (PCI) Data Security Standard – Report on Validation Reporting Instructions for PA-DSS v2.0 ("ROV Reporting Instructions")*
- *Payment Application Data Security Standard (PA-DSS) Attestation of Validation v2.02* ("AOV")

The latest 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")
- *Payment Card Industry (PCI) Data Security Standard Qualification Requirements for PA-QSAs ("PA-QSA Qualification Requirements")*

Note:

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

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

All of the above documents are available in electronic form on the Website.

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, e-mail 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.
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 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-QSAs and validation and Acceptance of Payment Applications, as further described in this document and related PCI SSC documents, policies and procedures.
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.

Term	Meaning
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 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.
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 Qualification Requirements	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) QSA Validation Requirements, PA-QSA Supplement*, or successor document (including if applicable, the *PCI QSA Qualification Requirements*) as published on the Website.
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 software 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

Term	Meaning
ROV	Report containing details documenting detailed results from an entity's PA-DSS Assessment for purposes of the PA-DSS Program.
Vendor (or vendor)	A vendor of a Payment Application.
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.

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 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:

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 by the Payment Card Brands to comply with the PCI DSS. Since Payment Applications are used to store, process, and transmit cardholder data, and entities are required 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 being 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.

1.7 Roles and Responsibilities

The following defines the roles and responsibilities of the stakeholders in the Payment Application community.

1.7.1 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.

1.7.2 PCI Security Standards Council (PCI SSC)

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, Minor 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.*

1.7.3 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 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, resellers, and integrators on how to install and configure the Payment Applications in a PCI DSS compliant manner;
- Ensuring their Payment Applications meet PA-DSS Requirements by successfully passing a PA-DSS Assessment as specified in *PCI PA-DSS Requirements and Security Assessment Procedures*;
- Complying with the *Vendor Release Agreement*;
- Creating a *PA-DSS Implementation Guide*, **specific to each application**, in accordance with the requirements in the *Payment Application Data Security Standard;* and

- Providing their customers (either directly or indirectly through their resellers and integrators) with a copy of the validated Payment Application's *PA-DSS Implementation Guide.* This includes any subsequent updates to the *PA-DSS Implementation Guide* that may result from changes to the Payment Application over time.

Vendors submit their Payment Applications and supporting documentation to the PA-QSA Company for review and authorize their PA-QSA Company to submit resulting ROVs and related information to PCI SSC.

1.7.4 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 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;
- Providing adequate documentation within the ROV to demonstrate the Payment Application's PA-DSS compliance;
- Submitting the ROV and/or any application 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.

1.7.5 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.

1.7.6 Qualified Integrators and Resellers (QIRs)

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.

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.*

1.7.7 Customers

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

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

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

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

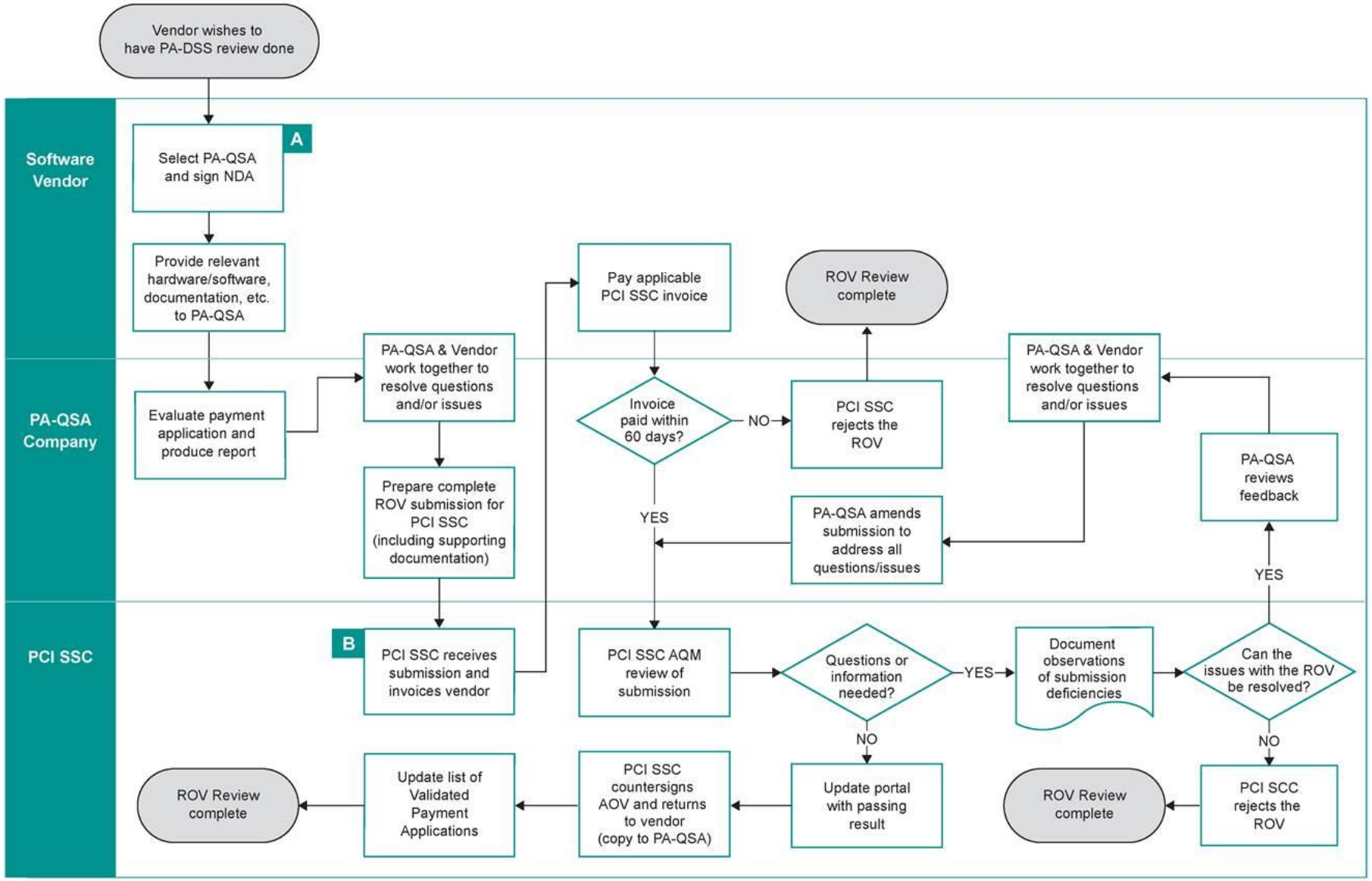
2 Overview of PA-DSS Validation Processes

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

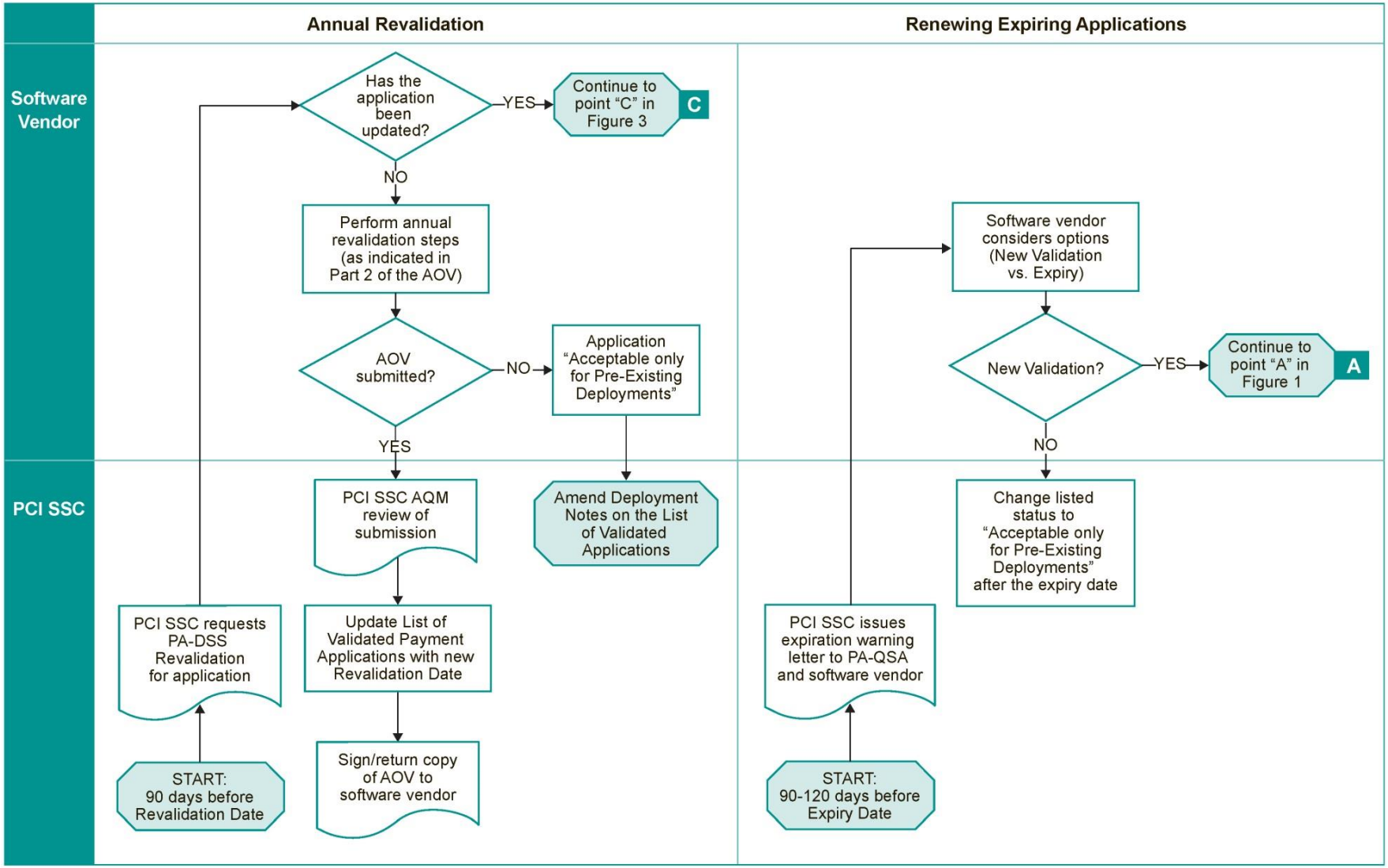
- The Vendor selects a PA-QSA Company from the Council's list of recognized PA-QSA Companies and negotiates the cost and any associated PA-QSA Company confidentiality and non-disclosure agreement with the PA-QSA Company;
- The Vendor then provides to the PA-QSA Company the Payment Application software, 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*;
- The PA-QSA Company then assesses the Payment Application, including its security functions and features, to determine whether the application complies with PA-DSS;
- 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*;
- 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 then 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
- 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 detail the following components of the PA-DSS Program:

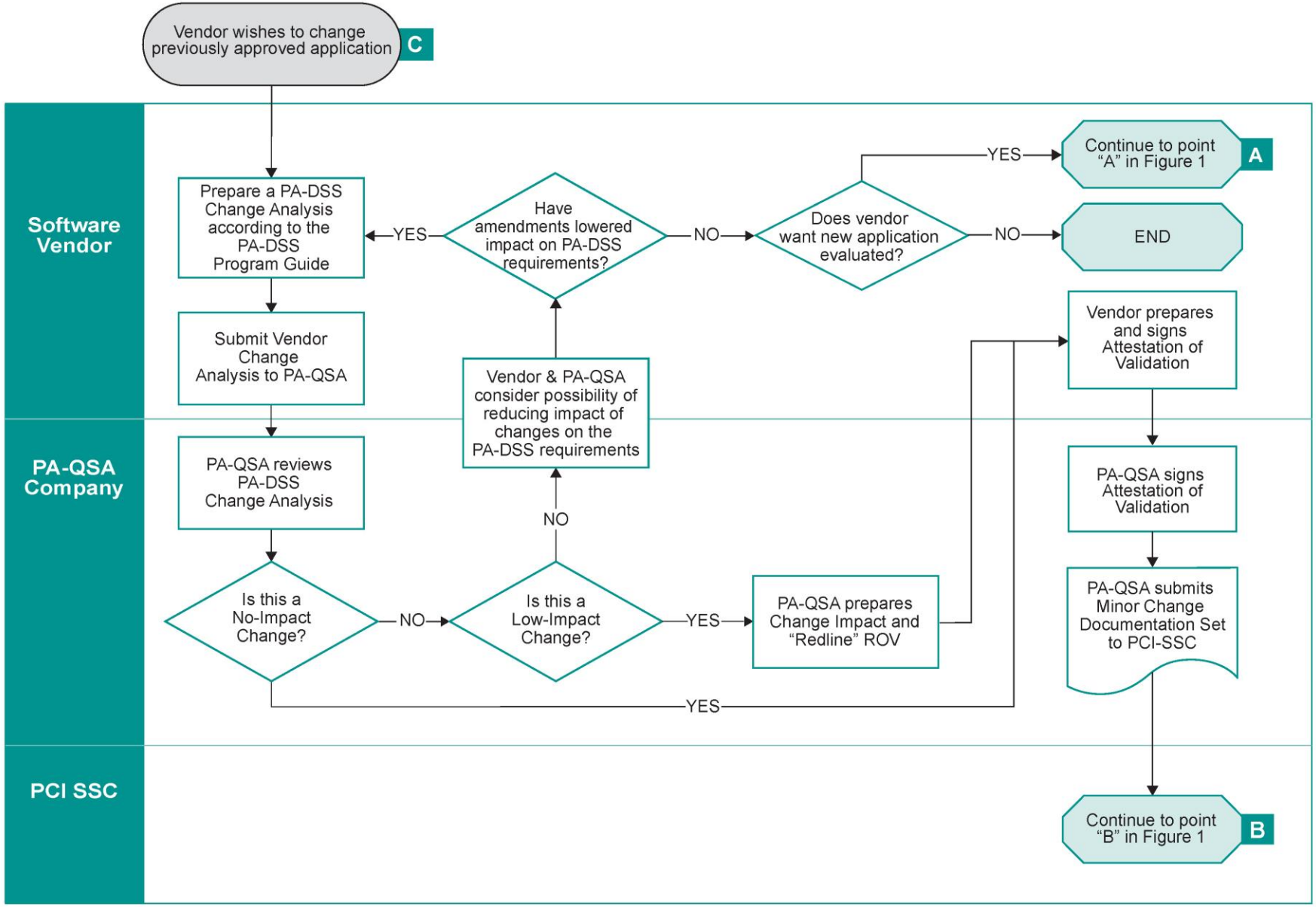
2.1 Figure 1: PA-DSS Report on Validation Submittal, Review, and Acceptance Process



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



2.3 Figure 3: PA-DSS Minor Updates to Listed Applications



3 Vendor Considerations – Preparation for the Review

3.1 To Which Applications Does PA-DSS Apply?

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

- PA-DSS does apply to Payment Applications that are typically sold and installed "off the shelf" without much customization by Vendors.
- PA-DSS does apply to 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 the only one performing payment functions (once confirmed by a PA-QSA Company). If other modules also perform payment functions, PA-DSS applies to those modules as well. Note that 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.
- PA-DSS does not apply to Payment Applications offered by application or service providers only as a service (unless such applications are also sold, licensed, or distributed to third parties) because:
  - 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;
  - The application is covered by the application or service provider's own PCI DSS review (this coverage should be confirmed by the customer); and/or
  - The application is not sold, distributed, or licensed to third parties.

  Examples of these "software as a service" Payment Applications include:

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

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

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

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

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

Note:

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

3.2 PA-DSS Applicability to Payment Applications on Hardware Terminals

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

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

1. The resident Payment Application directly meets all PA-DSS Requirements and is validated according to standard PA-DSS procedures; 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 in the "In Place" box for that Requirement;
3. Include a thorough explanation as to why the Payment Application could not meet the PA-DSS Requirement;
4. Document the procedures that were conducted to determine how that Requirement was fully met through a PCI PTS validated control; and
5. List the PCI PTS validated hardware terminal as a required dependency in the Executive Summary of the ROV.

Once the PA-QSA 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 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:

- Be provided together to the customer (both hardware terminal and application), OR, if provided separately, the application Vendor and/or the reseller/integrator must package the application for distribution such that it will only operate on the hardware terminal on which it has been validated to run;
- Enabled by default to support a customer's PCI DSS compliance;
- Include ongoing support and updates to maintain PCI DSS compliance; and
- 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.

3.3 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 PCI SSC website;
- Determine/assess the Payment Application's readiness to comply with PA-DSS:
  - Perform a "gap" analysis between how the Payment Application subject to PA-DSS functions compared to PA-DSS Requirements;
  - Correct any gaps;
  - 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 clean opinion, 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.

3.4 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 can be downloaded from the PCI SSC website. All completed Payment Application related materials such as install CDs, manuals, the *PA-DSS Implementation Guide*, the *Vendor Release Agreement* and all other materials related to the review and participation in the PA-DSS Program must be delivered to a PA-QSA Company listed on the PCI SSC website, 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* (note that this *must* be submitted to the PA-QSA Company);
   - Software Installation Guide or Instructions (as provided to customers);
   - Vendor's version-numbering scheme; and
   - Change control documentation that shows how changes are illustrated to customers;
5. Additional documentation—such as diagrams and flowcharts—that will aid in the Payment Application review (the PA-QSA Company may request additional material when necessary.); and
6. The Vendor's executed VRA.

3.5 PA-DSS Review Timeframes

The amount of time necessary for a PA-DSS Assessment, from the start of the 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 Company, 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).

3.6 Payment Application Qualified Security Assessors

PCI SSC qualifies and provides required training for Payment Application Qualified Security Assessor Companies and PA-QSA Employees to assess and validate Payment Applications for PA-DSS compliance. In order to perform PA-DSS Assessments, the 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.

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 its customer. Before deciding on a PA-QSA Company, it is recommended that a prospective customer should check PCI SSC's list of recognized PA-QSA Companies, talk to several PA-QSA Companies, and follow their own vendor-selection processes.

3.6.1 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 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 Assessment being rejected by PCI SSC.*

3.7 Technical Support throughout Testing

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

3.8 *Vendor Release Agreement* (VRA)

The Vendor's signed copy of the then-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-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-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.

3.9 The Portal

All documents relating to the Payment Application validation process are to be submitted by PA-QSA Companies, on behalf of the Vendor, to the Council through PCI SSC's secure web portal ("Portal").

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

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

3.10 PA-DSS Payment Application Acceptance Fees

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. PA-DSS 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.

4 Vendor Considerations – Managing a Validated Payment Application

4.1 Annual Revalidation

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

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

If an updated Attestation of Validation is not submitted for a listed Payment Application, that application will be deemed to have suffered an early administrative expiry. As such, the "Deployment Notes" on the List of Validated Applications *will be amended to identify that the Payment Application is "Acceptable only for Pre-Existing Deployments."*

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

The process flow for annual revalidation is detailed in Section 2.2, Figure 2.

4.2 Changes to Listed Payment Applications

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

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

1. **No Impact Changes** are minor changes (either administrative or software) made to a listed Payment Application that have no impact on the PA-DSS Requirements. In this case, for the new version to be listed, the Vendor documents the change for the PA-QSA Company's review—see Section 4.2.2, "No Impact Changes," for specifics. Examples of minor updates include, but are not limited to, corporate identity changes or software changes to a graphical user interface or to supporting modules that perform no Payment Application functions.
2. **Low Impact Changes** are minor changes made to a listed Payment Application that touch upon PA-DSS related functions of the Payment Application and have limited impact on the PA-DSS Requirements. In this case, for the new version to be accepted, the Vendor submits the new version of the Payment Application for a partial or "delta" review—see Section 4.2.3, "Low Impact Changes," for specifics.
3. **High Impact Changes** are changes made to a listed Payment Application that affect the PA-DSS related functions of the Payment Application and have a high impact on the PA-DSS Requirements. In this case, for the new version to be listed, the Vendor submits the new version of the Payment Application for a full PA-DSS review—see Section 4.2.4, "High Impact Changes," for specifics.

Examples of major updates include any changes that impact or change the functionality for PA-DSS Requirements or impact the security functioning of the Payment Application in a way that cannot be considered minor; including but not limited to, how the application stores, processes, or transmits PAN or sensitive authentication data, how users are authenticated, how PAN is rendered unreadable for storage or transmission, how logs are generated and managed, use of remote access, use of wireless technology, or changes to application infrastructure.

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

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

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

Note:

Minor Changes (No Impact or Low Impact) are only permissible to previously listed Payment Applications that have yet to expire.

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

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

The process flow for changes to listed applications is detailed in Section 2.3, Figure 3.

4.2.1 Change Documentation

4.2.1.1 Vendor Change Analysis Document

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

- Name of the Payment Application;
- Payment Application version number;
- Related Payment Application name and version number currently on the List of Validated Payment Applications;
- Description of the change;
- Indication of whether this is a *No Impact Change* or a *Low Impact Change* (see below);
- Description of why the change is necessary;
- Details of whether cardholder data and payment functions are impacted and what the impact is;
- Description of how the change functions;
- Description of testing performed by Vendor to validate that PA-DSS security requirements are not negatively impacted;
- Explanation of how and why PA-DSS Requirements are not negatively impacted;
- Description of how this change fits into Vendor's versioning methodology, including how this version number indicates that this is a "minor" change;
- If applicable, description of use of programming practices/module approaches and how such use prevents a negative impact to requirements; and
- The Vendor's updated *PA-DSS Implementation Guide*.

4.2.1.2 PA-QSA Company Change Impact Document

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

- A high-level description of each change that has been made to the Validated Payment Application
- Citations of:
  - The original ROV that and any subsequent Minor Changes (including No Impact and Low Impact Changes) upon which the current Minor Change is based; and
  - Any supporting documentation used to substantiate the findings represented in the *Vendor Change Analysis*;
- A table that depicts the following information about every change that is embodied in the Minor Change to the Validated Payment Application from the previously approved version:
  - A description of the change;
  - Identification of the amended configuration item or items (system files, modules, etc.) that is/are impacted by the change;
  - A high-level assessment by the PA-QSA Company of the security impact of the change;

- Identification of the PA-DSS Requirements or test procedures that are impacted by the change;
- Indication whether or not the impacted PA-DSS Requirements necessitated an update to the ROV (the "Redline" ROV would have the detail of the changes); and
- A high-level description of the testing completed, if any, used to validated the assessment;

4.2.2 No Impact Changes

4.2.2.1 Vendor Change Analysis & PA-QSA Company Concurrence is Required

There are two types of No Impact Changes:

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

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

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

i. The PA-QSA Company must so notify the Vendor;

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

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

iv. PCI SSC then issues an invoice to the Vendor for the applicable Change Fee; and

v. Upon payment of the invoice PCI SSC will review the *Attestation of Validation* and *Vendor Change Analysis* for quality assurance purposes.

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 the PA-DSS related functions of the Payment Application, the PA-QSA Company should return the *Vendor Change Analysis* to the Vendor and work with the Vendor to consider what actions are necessary to address the PA-QSA Company's observations.

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

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

ii. Sign and return a copy of the *PA-DSS Attestation of Validation* to both the Vendor and the PA-QSA Company. The expiry date of this newly listed application and version number will be the same as that of the "parent" Payment Application.

For quality issues associated any aspect of the submission, PCI SSC communicates those issues to the PA-QSA Company, and those issues are resolved according to the process depicted in Section 2.1, Figure 1. PCI SSC reserves the right to reject any *Vendor Change Analysis* if it determines that a change described therein and purported to be a No Impact Change by the PA-QSA Company or Vendor is ineligible for treatment as a No Impact Change.

4.2.3 Low Impact Changes

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

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

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

i. Inclusion of minor updates or patches to supported OS versions upon which the Payment Application was previously validated;

ii. Inclusion of minor updates or patches to supported third-party databases with which the Payment Application was previously validated;

iii. Updates to reporting modules;

iv. Additions or deletions of supported payment processors;

v. Inclusion of minor updates or patches to supported middleware with which the Payment Application was previously validated; and

vi. Recompilation of unchanged code base with either the same compiler using different flags or with a completely different compiler.

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

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

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

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

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

i. The PA-QSA Company must so notify the Vendor;

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

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

iv. The PA-QSA Company signs its 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 Company Change Impact document, to PCI SSC; and

v. PCI SSC then issues an invoice to the Vendor for the applicable Change Fee; and

vi. Upon payment of the invoice PCI SSC will review the *Attestation of Validation*, the "Redline" version of the ROV and the PA-QSA Company Change Impact document for quality assurance purposes.

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

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

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

ii. Sign and return a copy of the Attestation of Validation to both the Vendor and the PA-QSA Company. The expiry date of this newly listed application and version number will be the same as that of the "parent" Payment Application.

For quality issues associated any aspect of the submission, PCI SSC communicates those issues to the PA-QSA Company, and those issues are resolved according to the process depicted in Section 2.1, Figure 1. PCI SSC reserves the right to reject any *PA-QSA Company 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.

4.2.4 High Impact Changes

4.2.4.1 Full PA-DSS Assessment is required

If changes to the Payment Application do impact PA-DSS Requirements and are ineligible for treatment as a *Low Impact Change*, the Payment Application must undergo another full PA-DSS Assessment. The PA-QSA 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.

4.3 Renewing Expired Applications

As an application approaches its expiration date, PCI SSC will notify the Vendor of the pending expiration. The two options available for Vendor consideration are either new validation or expiry:

- **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 Minor Change process to achieve this goal is not permitted.

- **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, it retains its status on the List of Validated Applications as "Acceptable for New Deployments" and is assigned a new expiry date.

The process flow for renewing expired applications is detailed in Section 2.3, Figure 3.

4.4 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 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 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.

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

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

4.5.1 Notification and Timing

Notwithstanding any other legal obligations the Vendor may have, the Vendor must promptly notify PCI SSC of any Security Issue relating to any of the Vendor's listed Payment Applications.

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

Note:

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

4.5.2 Notification Format

The Vendor's formal notification to PCI SSC must be in writing in accordance with the *Vendor Release Agreement*, and should be preceded by a phone call to the PCI PA-DSS Program Manager at (781) 876-8855.

4.5.3 Notification Details

As part of the Vendor's initial notification to PCI SSC, the Vendor must supply the PCI SSC PA-DSS Program Manager with 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.

4.5.4 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 of the application in question about the Security Issue and, where possible, share information relating to the Security Issue.
- Support the Vendor's efforts to 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.

4.5.5 Withdrawal of Acceptance

PCI SSC reserves the right to suspend, withdraw revoke, cancel or place conditions upon its Acceptance of (and accordingly, remove from the *List of PA-DSS Validated Payment Applications*) any listed Payment Application in accordance with the 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, (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.

5 PA-QSA Company Reporting Considerations

5.1 PA-DSS Report Acceptance Process Overview

The PA-QSA Company performs the Payment Application review according to the *PA-DSS Security Assessment Procedures*, and produces a ROV that is shared with the Vendor. If the ROV has all items "in place," then the PA-QSA 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 highlighted in the ROV. For example, this may include updating user documentation or updating the 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, 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 PA-DSS Program materials), PCI SSC will send a PA-DSS *Attestation of Validation*, countersigned by PCI SSC, to both the Vendor and the PA-QSA Company, and then adds the application to the List of Validated Payment Applications.

For quality issues associated with ROVs, PCI SSC communicates those issues with the PA-QSA Company. It is then 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 to updating the ROV to reflect adequate documentation to support the PA-QSA Company's decisions. However, if the issues require that the PA-QSA Company perform more testing, the PA-QSA Company must notify the Vendor that re-testing is needed and schedule that testing with the Vendor.

The process flows for ROV Acceptance and ROV Review Process are detailed in Section 2.1, Figure 1.

5.2 Delivery of the ROV and Related Materials

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

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

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

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

5.2.1 Access to the Portal

Once a PA-QSA Company has had its first employee successfully complete the individual PA-QSA Employee certification process, PCI SSC will send login credentials and instructions for use of the Portal to the company's Primary PA-QSA Employee. Additional credentials can be requested by each company's Primary PA-QSA Employee 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.

5.2.2 New Applications

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

- *Vendor Release Agreement* signed by the Vendor
- ROVs completed in accordance with the ROV Reporting Instructions which contains the following information:
  - Executive Summary (Includes Reseller/Integrator List)
  - Requirements – Testing Procedures
  - PA-DSS v2.0, Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment
  - *Attestation of Validation* (AOV) signed by both the Vendor and the PA-QSA Company of Record
- *Implementation Guide* for the Payment Application assessed

5.2.3 Resubmissions

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

5.2.4 No Impact Changes

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

- Vendor Change Analysis document;
- Updated Vendor Release Agreement, if applicable;
- Updated *PA-DSS Implementation Guide* for the assessed Payment Application; and
- *Attestation of Validation* signed by both the Vendor and the PA-QSA Company.

5.2.5 Low Impact Changes

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

- PA-QSA Company's Change Impact document;
- Updated *PA-DSS Implementation Guide* for the assessed Payment Application;
- Updated ROV which contains the following:
  - Summary of requirements assessed and any resulting changes;
  - Updated Executive Summary and Requirement with edits clearly identified (i.e. "redlined"); and
  - Confirmation of Testing Laboratory (PA-DSS Appendix B); and
- *Attestation of Validation* signed by both the Vendor and the PA-QSA Company.

5.3 PA-DSS Reporting Processes

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

- PCI SSC shall review the ROV (generally within 30 calendar days of payment of invoice) and determine if it is acceptable.
- If no issues or questions to the PA-QSA Company are identified, PCI SSC will issue the *Attestation of Validation*, countersigned by PCI SSC, post the Payment Application and Vendor's information to the Website, and the application is thereby Accepted.
- If questions or issues are identified and sent to the PA-QSA Company, the process described above will restart upon receipt of a complete and acceptable revised ROV or response ("Revised ROV") from the PA-QSA Company. PCI SSC reserves the right to ask for additional supporting documentation that may be necessary to substantiate the findings documented in the ROV. The process re-start does not occur until receipt of an acceptable Revised ROV addressing all previously identified items. PCI SSC will generally review a Revised ROV within 30 calendar days of receipt.
- Should additional questions or issues arise, the cycle repeats until a satisfactory Revised ROV is received, at which time, PCI SSC will issue the *Attestation of Validation*, post the information to the PCI SSC website, and the application is thereby Accepted. Additional issues or questions may be raised at any time prior to Acceptance.
- ROVs that have been returned to the PA-QSA Company for correction must be resubmitted to the PCI SSC within 30 days. 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 submission.

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

The listing on the List of Validated Payment Applications will contain, at minimum, the information specified below. Each characteristic is detailed in Appendix A: Elements for the *Attestation of Validation* and 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 (PABP or PA-DSS version)
- Deployment Notes
- Revalidation Date
- Expiry Date
- PA-QSA Company

***Note**:*

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

5.4 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 Section 5.5, Figure 4.

5.4.1 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.

5.4.2 PA-QSA Company 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.

5.4.3 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.*

5.4.3.1 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.

5.4.3.2 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:

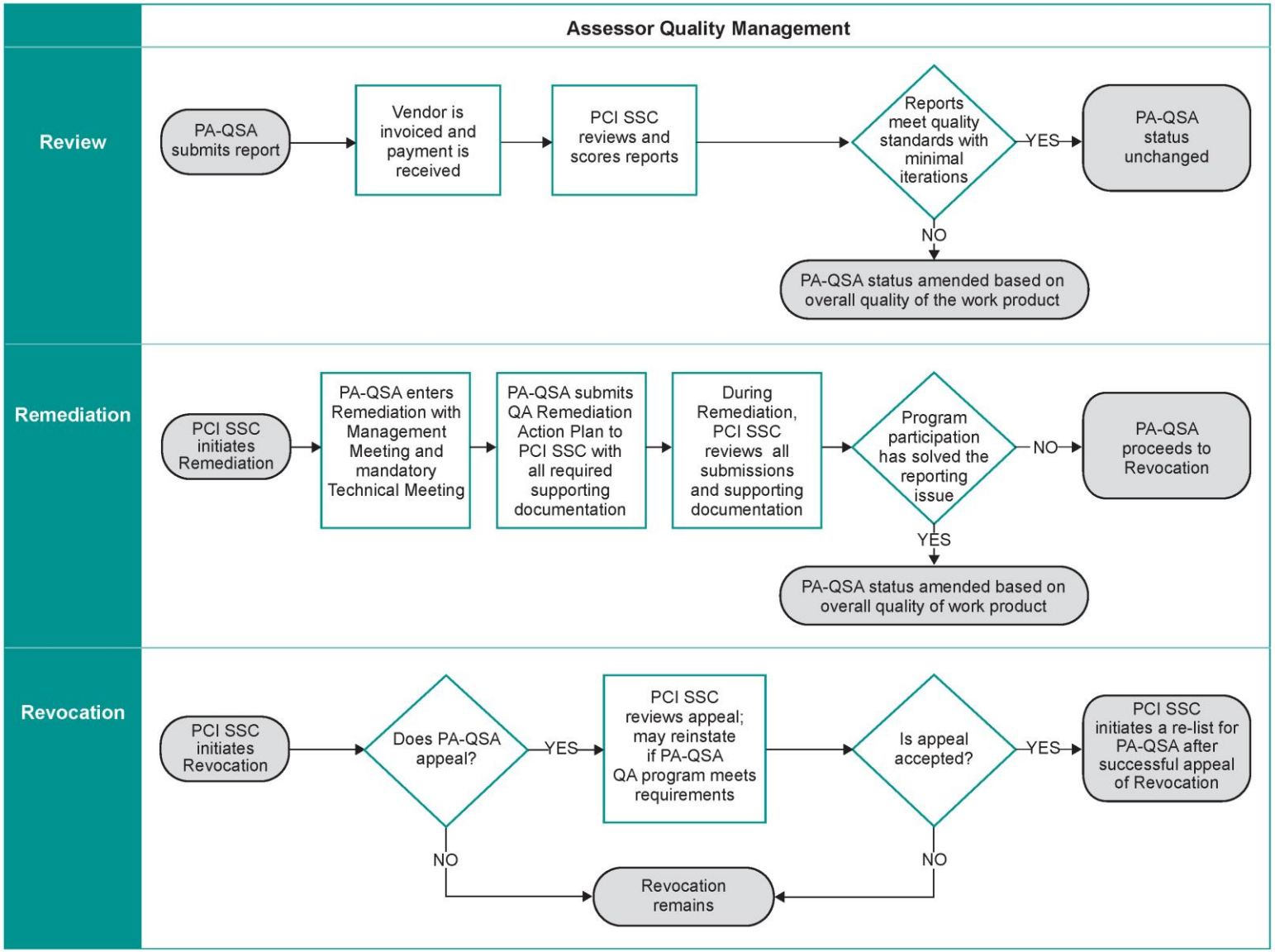
If a Payment Application included on the PCI SSC List of PA-DSS Validated Payment Applications is compromised due to PA-QSA Company and/or Employee error, then that PA-QSA Company and/or Employee may immediately be placed into Remediation or its status revoked.

5.4.3.3 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.

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



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

6 Legal Terms and Conditions

Acceptance of a given Payment Application by the PCI Security Standards Council LLC (PCI SSC) only applies to the specific version of that Payment Application that was reviewed by a PA-QSA Company and subsequently accepted by PCI SSC (the Accepted Version). If any aspect of a Payment Application or version thereof is different from that which was reviewed by the PA-QSA and Accepted by PCI SSC—even if the different Payment Application or version (the Alternate Version) conforms to the basic product description of the Accepted Version—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 issued an *Attestation of Validation* provided by PCI SSC. All other references to PCI SSC's Acceptance or Approval of a Payment Application or version thereof are strictly and actively prohibited by PCI SSC.

PCI SSC Acceptance signifies that (i) a PA-QSA has determined that 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 Brand.

.

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

A.1 Payment Application Vendor

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

A.2 Payment Application Identifier

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

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

Example of a Payment Application Identifier:

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

Example of a Payment Application Identifier:

- **Payment Application Name**

  Payment Application Name is provided by the Vendor, and is the name by which the Payment Application is sold.

- **Payment Application Version #**

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

  Note:

  In PA-DSS, see Instructions and Content for Report on Validation section for details about content to include in the PA-DSS ROV for Vendor's versioning methods.

  Customers are strongly advised to purchase and deploy only those Payment Applications with the Application Version # whose characters match exactly the Application Version # shown on the List of Validated Payment Applications.

- **Payment Application Type**

  The Payment Application type denotes the major categories of payment functions performed by Payment Applications, and consists of the following:

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

Type	Function	Description
12	Payment Module	Payment software that operates as a component of a broader application environment upon which it is dependent to operate. Such software must have distinguishable configuration identifiers that are easily discernable 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 version	3 alpha characters (assigned as received)

A.3 Description Provided by Vendor

This section allows for the submission of a description of the Payment Application that is to be used in the List of Validated Payment Application should the ROV be accepted. 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 that the application was tested on.

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 re-validation, whether or not the particular version of the Payment Application is still being supported by the Vendor, or by the Payment Application's Expiration Date (noted below).

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

1. **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 (i) annual revalidation requirements are not maintained by the Vendor causing an administrative early expiry, or (ii) the Validated Payment Application expires as a matter of course based on the version of the PA-DSS under which it was validated.
2. **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 administrative early expiry, or (ii) the Validated Payment Application expires as a matter of course based on the version of the PA-DSS under which it was validated. 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 is 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 get the application re-evaluated against the current PA-DSS Requirements in order to maintain the acceptance. The Expiry Date is related to the Deployment Notes, noted above.

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

For example: Payment Applications validated against PA-DSS Version 2.0 will have an expiration date of 2016 as PA-DSS version 3.0 was released in October 2013; while reviews against PA-DSS Versions 1.2 expired in October 2013.

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

Validation Notes	Expiry Date	Deployment Notes	Annual Revalidation Required
Validated According to PA-DSS (PA-DSS v2.0)	28 October 2016	Acceptable for New Deployments	Yes
Validated According to PA-DSS (PA-DSS v1.2.1, v1.2, or v1.1)	28 October 2013	Acceptable 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: 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-QSAs to work together to develop methods to certify and digitally sign Payment Application builds. PCI SSC reserves the right to require certified application builds in the future.

For example, such a method could include the following:

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