Payment Card Industry (PCI)

Payment Application Data Security Standard (PA-DSS)

Program Guide

Version 1.2.1

July 2009

Document Changes

<table>
<tr><th>Date</th><th>Version</th><th>Description</th></tr>
<tr><td>October 1, 2008</td><td>1.2</td><td>To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.</td></tr>
<tr><td rowspan="11">July 2009</td><td rowspan="11">1.2.1</td><td>Minor corrections to version 1.2 as follows:
<table>
<tr><th>Description</th><th>Pages</th></tr>
<tr><td>In “To which Applications does PA-DSS Apply?” section, provide further clarity about what is considered a "payment application."</td><td>9</td></tr>
<tr><td>Add reference to the new PA-DSS Listing Summary, in “Related Publications” and “Release Agreement and Delivery of Report” sections. The PA-DSS Listing Summary is for PA-QSAs to submit with report, to specify report and listing information for PCI SSC to use. The form is not included in PA-DSS Program Guide but is available at https://www.pcisecuritystandards.org/security_standards/pci_pa_dss.shtml.</td><td>4 & 12</td></tr>
<tr><td>Add fraud-scoring or detection applications as examples of non-payment applications that may be part of a payment application suite.</td><td>9</td></tr>
<tr><td>Clarify language in “Fees” section to eliminate previous “quarterly” wording, add annual maintenance fee of $500, clarify that grandfathered PABP applications will be charged a one-time fee of $1250 (rather than an annual fee), add reference to Figure 4 for details about renewing expired applications, and add a $125 listing fee for minor updates.</td><td>13</td></tr>
<tr><td>Add column to the table of figures, to refer to page numbers with additional Program Guide content related to each figure.</td><td>14</td></tr>
<tr><td>Change terminology used previously for changes to listed payment applications to “minor update” in “Overview of PA-DSS Processes,” Figure 2, and “Changes to Listed Payment Applications”; added terms “major update,” “minor update,” and “no update.” Clarified process in “Minor Update – No Impact to PA-DSS Requirements.” Changed title related to self-attestation form in Appendix C to “Self-Attestation for Minor Update.”</td><td>16, 21, 22, 37</td></tr>
<tr><td>Changed “Not acceptable for new deployments” to “Acceptable only for pre-existing” deployments.”</td><td>17, 18. 23, 24, 35</td></tr>
<tr><td>In “PA-DSS Report Acceptance Process Overview” section, changed “release agreement” to “vendor release agreement” to match language in “Legal Terms and Conditions” section.</td><td>20</td></tr>
<tr><td>In “Renewing Expired Applications” section, added second sentence to Item 2.</td><td>23</td></tr>
<tr><td>Clarify language in sections for “Payment Applications undergoing PABP Reviews During Transition” and “PA-DSS Transition Procedures.” Deleted part of footnote that referred to PABP 1.4 and the October 15, 2008 date, since the date is past. Clarify that PCI SSC will not accept PABP Transition Procedures after September 30, 2009.</td><td>24, 25</td></tr>
</table></td></tr>
</table>

Document Changes *(continued)*

Date	Version	Description	Pages
July 2009	1.2.1	In “PA-DSS Reporting Processes” section and *Appendix A*, clarify process and change language used for contents of List of Validated Payment Applications to match language used in posted list. Expanded *Appendix A* to include tables with details about payment application types and the reference number.	28, 32
		In section formerly called “Notification Following a Security Breach or Compromise,” add "vulnerability" throughout—now the language is "security breach, compromise, or known vulnerability."	29
		Change language in “Legal Terms and Conditions” section to match that currently included in the *PA-DSS Vendor Release Agreement.*	31

Table of Contents

Document Changes **1**

Introduction **4**

Related Publications 4
Updates to Documents and Security Requirements 4
Terminology 4
About PCI 5
PA-DSS Alignment Initiative and Overview 5
Roles and Responsibilities 5

Vendor Considerations – Preparation for the Review **9**

To Which Applications does PA-DSS Apply? 9
PA-DSS Applicability to Hardware Terminals 10
Prior to the Review 10
Required Documentation and Materials 11
PA-DSS Review Timeframes 11
Payment Application Qualified Security Assessors 12
Related PA-DSS services that may be offered by PA-QSAs 12
Technical Support throughout Testing 12
Release Agreement and Delivery of Report 12
Fees 13

Overview of PA-DSS Processes **14**

Figure 1: PA-DSS Report Acceptance Process 15
Figure 2: PA-DSS Minor Updates to Listed Applications 16
Figure 3: Grandfathering and Transitioning PABP Applications to PA-DSS List 17
Figure 4: PA-DSS Annual Revalidation and Renewing Expired Applications 18
Figure 5: PA-QSA QA Programs for Report Reviews 19

PA-DSS Report Acceptance Process Overview **20**

Changes to Listed Payment Applications **21**

Renewing Expired Applications **23**

Transition and Grandfathering of PABP-validated Payment Applications **24**

Quality Assurance Program **26**

PA-DSS Reporting Processes **28**

Notification Following a Security Breach, Compromise, or Known Vulnerability **29**

Legal Terms and Conditions **31**

Appendix A: Elements for Acceptance Letter and *List of Validated Payment Applications* **32**

Appendix B: Identification of Certified Payment Application Builds **36**

Appendix C: Self-Attestation for Minor Update **37**

Introduction

Related Publications

The following documents are the basis for payment application assessments:

- *Payment Card Industry (PCI) Payment Application Data Security Standard – Requirements and Security Assessment Procedures*
- *Payment Card Industry (PCI) Payment Application Data Security Standard – Transition Procedures*

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

- *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures*
- *Payment Card Industry (PCI) Data Security Standard and Payment Application Data Security Standard Glossary of Terms, Abbreviations, and Acronyms*
- *Payment Card Industry (PCI) Data Security Standard QSA Validation Requirements*
- *Payment Card Industry (PCI) Data Security Standard QSA Validation Requirements – Supplement for Payment Application Qualified Security Assessors (PA-QSAs)*
- *Payment Card Industry (PCI) Payment Application Data Security Standard Listing Summary*

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 to validate the payment application's compliance and document the review.*

The two QSA Validation Requirements documents define the requirements that must be met by a PA-QSA in order to perform assessments.

The PA-DSS Listing Summary *solicits contact and additional information to support the listing of a payment application on the Website once it has been approved by PCI SSC.*

PCI Data Security Standard Requirements and Security Assessment Procedures *are the foundation for all the afore-mentioned. All documents are available in electronic form on www.pcisecuritystandards.org.*

Updates to Documents and Security Requirements

Security is a never-ending race against potential attackers. As a result, it is necessary to regularly review, update and improve the security requirements used to evaluate payment applications. As such, PCI SSC will endeavour to update payment application security requirements every 24 months.

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

Terminology

Throughout this document:

- "PCI SSC" refers to the PCI Security Standards Council, LLC.
- "PABP" will mean Visa's former Payment Application Best Practices program, upon which the Payment Application Data Security Standard ("PA-DSS") was based.
- "Payment brands" refers to the payment card brands that are members of PCI SSC, currently American Express, Discover, JCB, MasterCard, and Visa.
- "Payment Applications" refer broadly to all payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.

About PCI

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

All stakeholders in the payments value chain benefit from the aligned requirements:

- Customers benefit from a broader selection of secure payment applications.
- Customers are assured that they will be using products that have met the required level of validation.
- Vendors will only be required to complete a single payment application review that will be recognized by all payment brands.

For more information regarding PCI SSC, see the PCI SSC's website at www.pcisecuritystandards.org (the "Website").

PA-DSS Alignment Initiative and Overview

This Payment Card Industry PA-DSS Program Guide reflects an alignment of the payment brands' requirements to a standard set of:

- Payment application security requirements and assessment procedures
- Processes for recognizing payment applications validated by PA-QSAs
- Processes for PABP-validated payment applications to transition to the PCI SSC list
- Quality assurance processes for PA-QSAs

Note:

PA-DSS reports are reviewed and recognized directly by PCI SSC.

Traditional PCI DSS compliance may not apply directly to payment application vendors since most vendors do not store, process, or transmit cardholder data. However, since these payment applications are used by customers to store, process, and transmit cardholder data, and customers are required to be PCI DSS compliant, payment applications should facilitate, and not prevent, the customers' PCI DSS compliance. Examples of how payment applications can prevent PCI DSS compliance include.

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

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

Roles and Responsibilities

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

The following defines the roles and responsibilities of the stakeholders in the payment application community. Those stakeholders that are involved in the assessment process have those related responsibilities listed.

Payment Brands

American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. are the payment brands that founded the PCI SSC. These payment brands are responsible for developing and enforcing any programs related to PA-DSS compliance, including, but not limited to, the following:

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

The payment brands may define compliance programs, mandates, dates, etc. using PA-DSS and the validated payment applications listed by PCI SSC. Through these compliance programs, the payment brands promote use of the listed validated payment applications.

Payment Card Industry Security Standards Council (PCI SSC)

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

- Is a centralized repository for PA-DSS Reports of Validation (ROVs)
- Performs Quality Assurance (QA) reviews of PA-DSS ROVs to confirm report consistency and quality
- Lists PA-DSS validated payment applications on the Website. *Note that this list will not be available on the Website until after October 2008.*
- Qualifies and trains PA-QSAs to perform PA-DSS reviews
- Maintains and updates the PA-DSS standard and related documentation according to a standards lifecycle management process.

Note that PCI SSC does not approve reports from a validation perspective. The role of the PA-QSA is to document the payment application's compliance to the PA-DSS as of the date of the assessment. Additionally, PCI SSC performs QA to assure that the PA-QSAs accurately and thoroughly document PA-DSS assessments.

Software Vendors

Software vendors ("vendors") develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, and then sell, distribute, or license these payment applications to third parties (customers or resellers/integrators). 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 PCI DSS requirements whenever the vendor stores, processes or transmits cardholder data (for example, during customer troubleshooting)
- Creating a *PA-DSS Implementation Guide*, specific to each application, according to the requirements in the *Payment Application Data Security Standard*
- Educating customers, resellers, and integrators on how to install and configure the payment applications in a PCI DSS-compliant manner.
- Ensuring payment applications meet PA-DSS requirements by successfully passing a PA-DSS review as specified in *PCI PA-DSS Requirements and Security Assessment Procedures.*

Vendors submit their payment applications and supporting documentation to the PA-QSA for review. Any agreements and costs associated with the assessment are negotiated between the vendor and the PA-QSA. Vendors provide permission for their PA-QSA to submit resulting PA-DSS compliance reports to PCI SSC.

PA-QSAs

PA-QSAs are QSAs that have been qualified and trained by PCI SSC to perform PA-DSS reviews. *Note that all QSAs are not PA-QSAs – there are additional qualification requirements that must be met for a QSA to become a PA-QSA.*

PA-QSAs are responsible for:

- Performing assessments on payment applications in accordance with the Security Assessment Procedures and the PA-QSA Validation Requirements
- Providing an opinion regarding whether the payment application meets PA-DSS requirements
- Providing adequate documentation within the ROV to demonstrate the payment application's compliance to the PA-DSS
- Submitting the ROV to PCI SSC, along with the Attestation of Validation (signed by both PA-QSA and vendor)
- Maintaining an internal quality assurance process for their PA-QSA efforts

It is the PA-QSA's responsibility to state whether the payment application has achieved compliance. PCI SSC does not approve ROVs from a technical compliance perspective, but performs QA reviews on the ROVs to assure that the reports adequately document the demonstration of compliance.

Resellers and Integrators

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

- Implementing only PA-DSS compliant 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 *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.

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

Customers

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

Note:

A PA-DSS compliant payment application alone is no guarantee of PCI DSS compliance.

- Implementing a PA-DSS-compliant payment application into a PCI DSS-compliant environment;
- Configuring the payment application (where configuration options are provided) according to the *PA-DSS Implementation Guide* provided by the vendor;
- Configuring the payment application in a PCI DSS-compliant manner;
- Maintaining the PCI DSS-compliant status for both the environment and the payment application configuration.

Once the list is posted by PCI SSC in the latter half of 2008, customers can find a listing of validated payment applications, along with other reference materials, on the Website.

Vendor Considerations – Preparation for the Review

To Which Applications does PA-DSS Apply?

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

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

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

  1) The application is a service offered to customers (typically merchants) and the customers do not have the ability to manage, install, or control the application or its environment;

  2) The application is covered by the application or service provider's own PCI DSS review (this coverage should be confirmed by the customer); and/or

  3) The application is not sold, distributed, or licensed to third parties.

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

  1) Those offered by Application Service Providers (ASP) who host a payment application on their site for their customers' use. Note that PA-DSS would apply, however, if the ASP's payment application is also sold to, and implemented on, a third-party site, and the application was not covered by the ASP's PCI DSS review.

  2) Virtual terminal applications that reside on a service providers' site and are used by merchants to enter their payment transactions. Note that PA-DSS would apply if the virtual terminal application has a portion that is distributed to, and implemented on, the merchant's site, and was not covered by the virtual terminal provider's PCI DSS review.
- PA-DSS does not apply to non-payment applications that are part of a payment application suite. Such applications (e.g., a fraud-monitoring, scoring, or detection application included in a suite) 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 only one 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.

The following list, while not all-inclusive, illustrates applications that are NOT payment applications for purposes of PA-DSS (and therefore do not need to undergo PA-DSS reviews):

- 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 list applications that are payment applications.

PA-DSS Applicability to Hardware Terminals

Hardware terminals with resident payment applications (also called dumb POS terminals or standalone POS terminals), do not need to undergo a PA-DSS review ***if all of the following are true*:**

- The terminal has no connections to any of the merchant's systems or networks;
- The terminal connects only to the acquirer or processor;
- The payment application vendor provides secure remote:
  1) Updates,
  2) Troubleshooting,
  3) Access, and
  4) Maintenance; and
- The following are never stored after authorization:
  - The full contents of any track from the magnetic stripe (that is, on the back of a card, in a chip, or elsewhere)
  - Card-validation code or value (three- or four-digit number printed on front or back of payment card)
  - PIN or encrypted PIN block

Prior to the Review

- Review both PCI DSS and PA-DSS requirements and related documentation located at the Website.
- Determine/assess 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 may perform a pre-assessment or "gap" analysis of a vendor's payment application. If the PA-QSA notes deficiencies that would prevent a clean opinion, the PA-QSA will provide to the software vendor a list of payment application features to be addressed before the formal review process begins.

- Determine whether *PA-DSS Implementation* Guide meets PA-DSS requirements.

Required Documentation and Materials

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

All information and documents relevant to the PA-DSS can be downloaded from the Website. All completed payment application related materials such as install CDs, manuals, the *PA-DSS Implementation Guide*, etc. related to performing the review must be delivered to a PA-QSA listed on the Website, not to PCI SSC. Review-specific information should be requested directly from the PA-QSA.

Examples of documents and items to submit to the PA-QSA include:

1. The payment application with operator's manual or instructions
2. The necessary hardware and software accessories to perform simulated payment transactions
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 fulfil this requirement.)
4. Documentation that relates to installing and configuring the application, or which provides information about the application. Examples of such documentation include:
    - *PA-DSS Implementation Guide*
    - Software Installation Guide or Instructions (as provided to customers)
    - Vendor's version-numbering scheme
    - Change control documentation that shows how changes are illustrated to customers
5. Additional documentation—such as diagrams and flowcharts—that will aid in the payment application review (the PA-QSA may request additional material when necessary.)

PA-DSS Review Timeframes

The amount of time necessary for a PA-DSS review, from start to completion resulting in a fully validated application with all items noted as "in place," can vary widely. Factors that determine the length of time include:

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

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

Payment Application Qualified Security Assessors

PCI SSC qualifies and trains Payment Application Qualified Security Assessors (PA-QSAs) to perform PA-DSS assessments. PA-QSAs are listed on the Website. These are the only assessors recognized by PCI SSC as able to perform PA-DSS assessments.

The prices and fees charged by PA-QSAs are not set by PCI SSC; these fees are negotiated between the PA-QSA and their customer. Before deciding on a PA-QSA, it is recommended that entities should talk to several PA-QSA firms, and follow their company's vendor selection processes.

Related PA-DSS services that may be offered by PA-QSAs

None of these services are required or recommended by PCI SSC. This list is included to provide examples of the types of services that may be offered by PA-QSAs. If these services are of interest to your company, please contact PA-QSAs for availability and pricing. Example PA-DSS related services include:

- Guidance on designing payment applications in accordance with PA-DSS
- Review of a software vendor's software design, response to questions via e-mail or phone, and participation in conference calls to clarify requirements
- Guidance on preparing the *PA-DSS Implementation Guide*
- Pre-assessment ("gap" analysis) services prior to beginning formal PA-DSS assessment
- Guidance for bringing the payment application into compliance with PA-DSS if gaps or areas of non-compliance are noted during the assessment

Technical Support throughout Testing

It is recommended that the vendor make 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.

Release Agreement and Delivery of Report

Prior to the PA-QSA releasing the PA-DSS report to PCI SSC, the vendor must sign PCI SSC's *Payment Card Industry PA-DSS Vendor Release Agreement* (the "Release Agreement"), giving permission for release of the report to PCI SSC for review. The Release Agreement **must be delivered directly** to PCI SSC by the PA-QSA, along with the PA-DSS reports. In addition, the PA-QSA must complete and submit the *PA-DSS Listing Summary*, which is posted at https://www.pcisecuritystandards.org/security_standards/pci_pa_dss.shtml.

Fees

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

Vendors will be assessed a listing fee of US $1,250 for each new payment application added to the PCI SSC payment application list. Once an application is listed, vendors will be assessed a maintenance fee of US $500 per year to list the application until the stated application expiration date.

For PABP applications grandfathering to the PCI SSC payment application list, vendors will be assessed a one-time fee of $1250 to list the application until the stated application expiration date.

Note:

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

PCI SSC will bill the vendor for all listing fees and the vendor will pay these listing fees directly to PCI SSC.

If a listed payment application is revised, but the revision is minor and does not negatively impact security (refer to the Change Analysis process in the Minor Update section under "Changes to Listed Applications" on page 19 of this document), the fee to update the listing will be US $125 per year. An updated Acceptance Letter for a given Minor Update will be issued after payment of the corresponding initial Minor Update Listing Fee.

As part of the Annual Revalidation process, the maintenance fee will be billed annually by PCI SSC to software vendors for all payment applications listed by PCI SSC for that vendor on the billing date. Vendors shall not be billed for applications that are validated but for which the software vendor chooses to not have the product listed on the Website. Note that vendors will not be allowed to manipulate listings to avoid the fee. I.e., vendors cannot have an application pulled from the listing and then request that it be re-listed after the billing.

See Figure 4 and the "Changes to Listed Payment Applications" section later in document for details about annual revalidation and renewing expired applications.

Overview of PA-DSS Processes

The PA-DSS review process is initiated by the vendor. The Website has all of the associated documents the vendor will need to navigate the PA-DSS review process. The vendor selects a PA-QSA from the PCI SSC list, and negotiates the cost and NDA with the PA-QSA. The vendor then provides the payment application software, manuals and other required documentation to the PA-QSA. PCI SSC will then issue an acceptance letter, confirming successful completion of the process for each payment application (a "PA-DSS Acceptance Letter"). Once the payment application is accepted, the product will be listed on the Website.

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

Process	Illustration	Page	Page Number for Related Section
PA-DSS Report Acceptance Process	Figure 1	15	20, 27
PA-DSS Minor Updates to Listed Applications	Figure 2	16	21
Grandfathering and Transitioning PABP Applications to PA-DSS List	Figure 3	17	24
PA-DSS Annual Revalidation and Renewing Expired Applications	Figure 4	18	22, 23
PA-QSA QA Program for Report Reviews	Figure 5	19	26

Figure 1: PA-DSS Report Acceptance Process

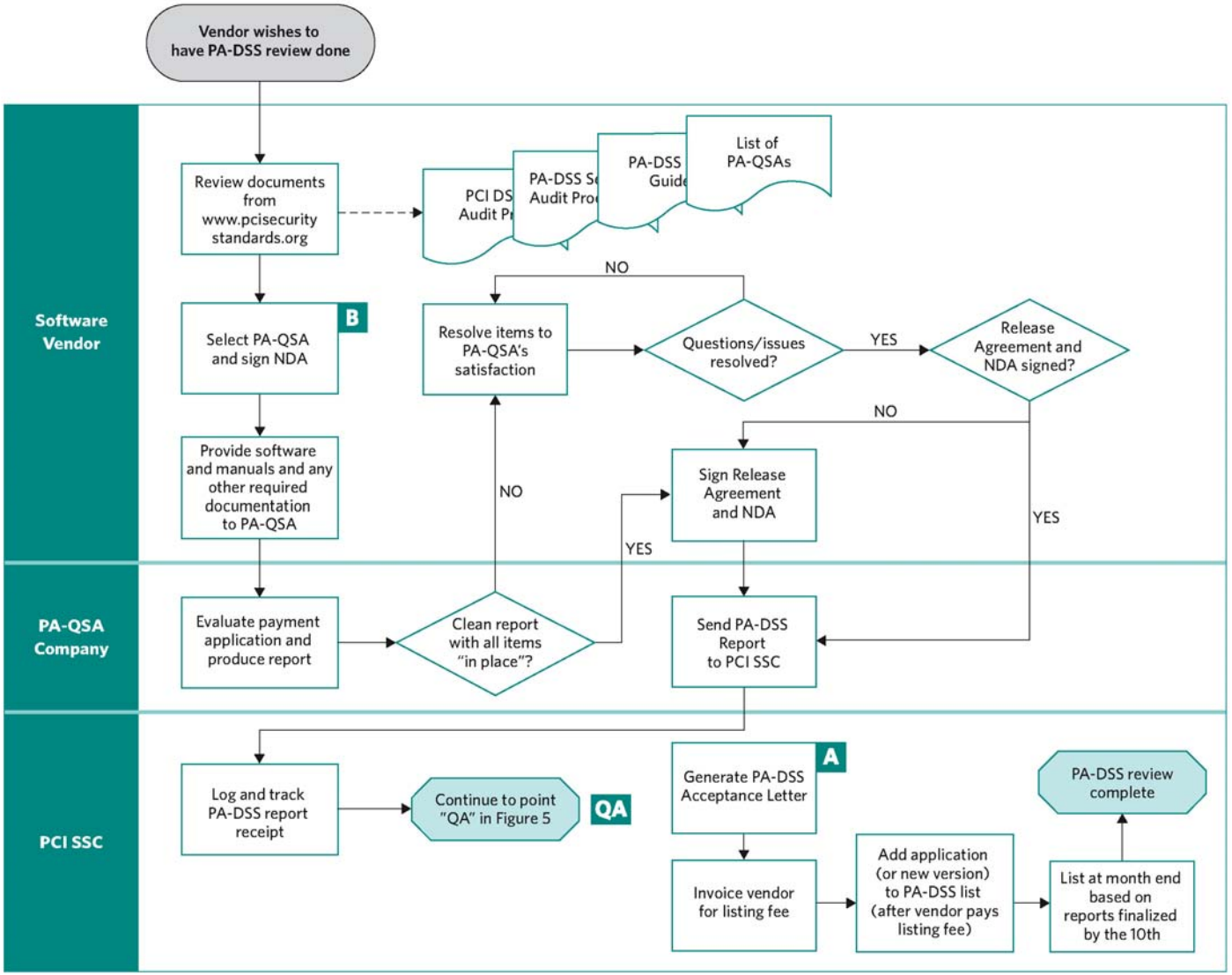


Figure 2: PA-DSS Minor Updates to Listed Applications

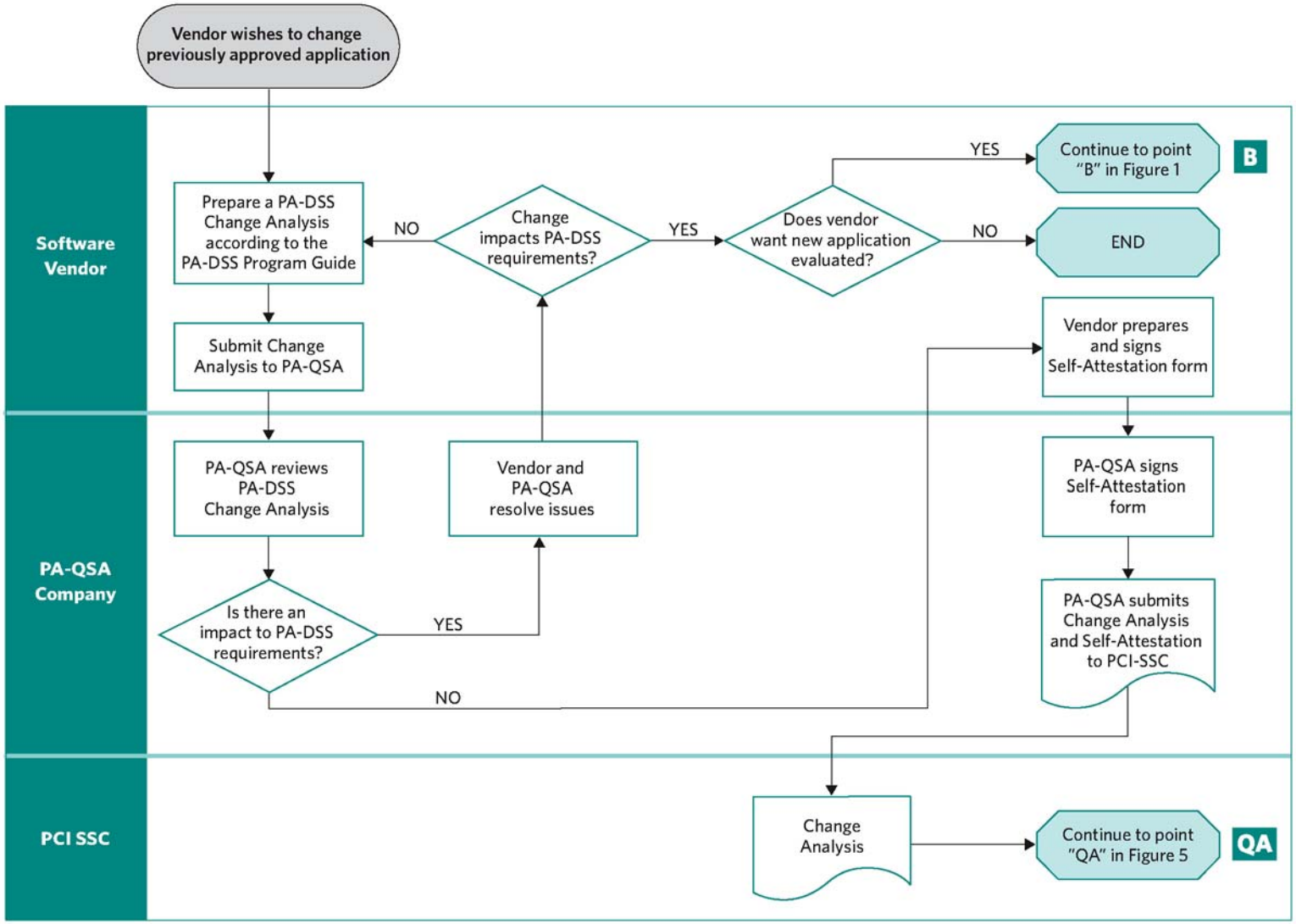


Figure 3: Grandfathering and Transitioning PABP Applications to PA-DSS List

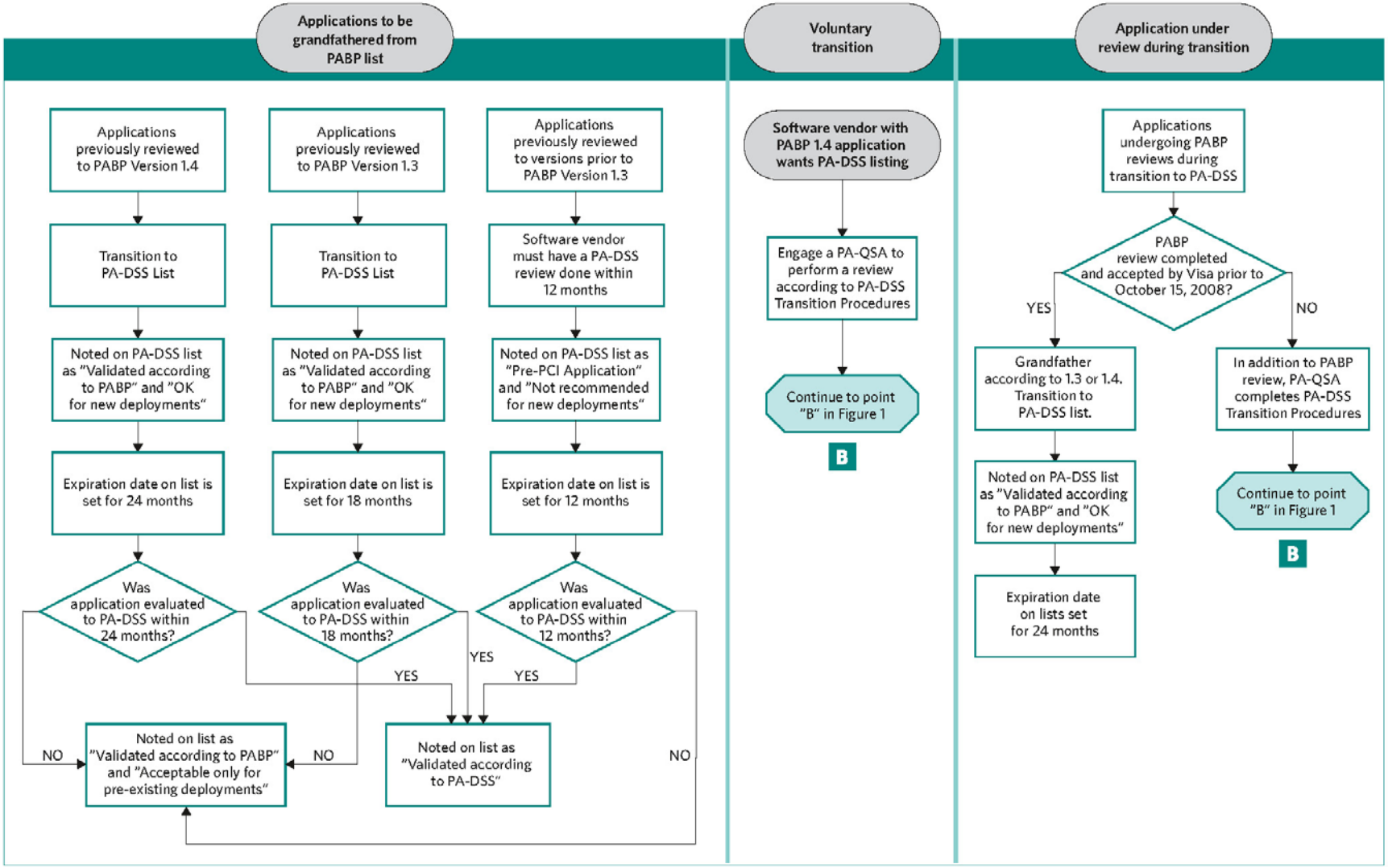


Figure 4: PA-DSS Annual Revalidation and Renewing Expired Applications

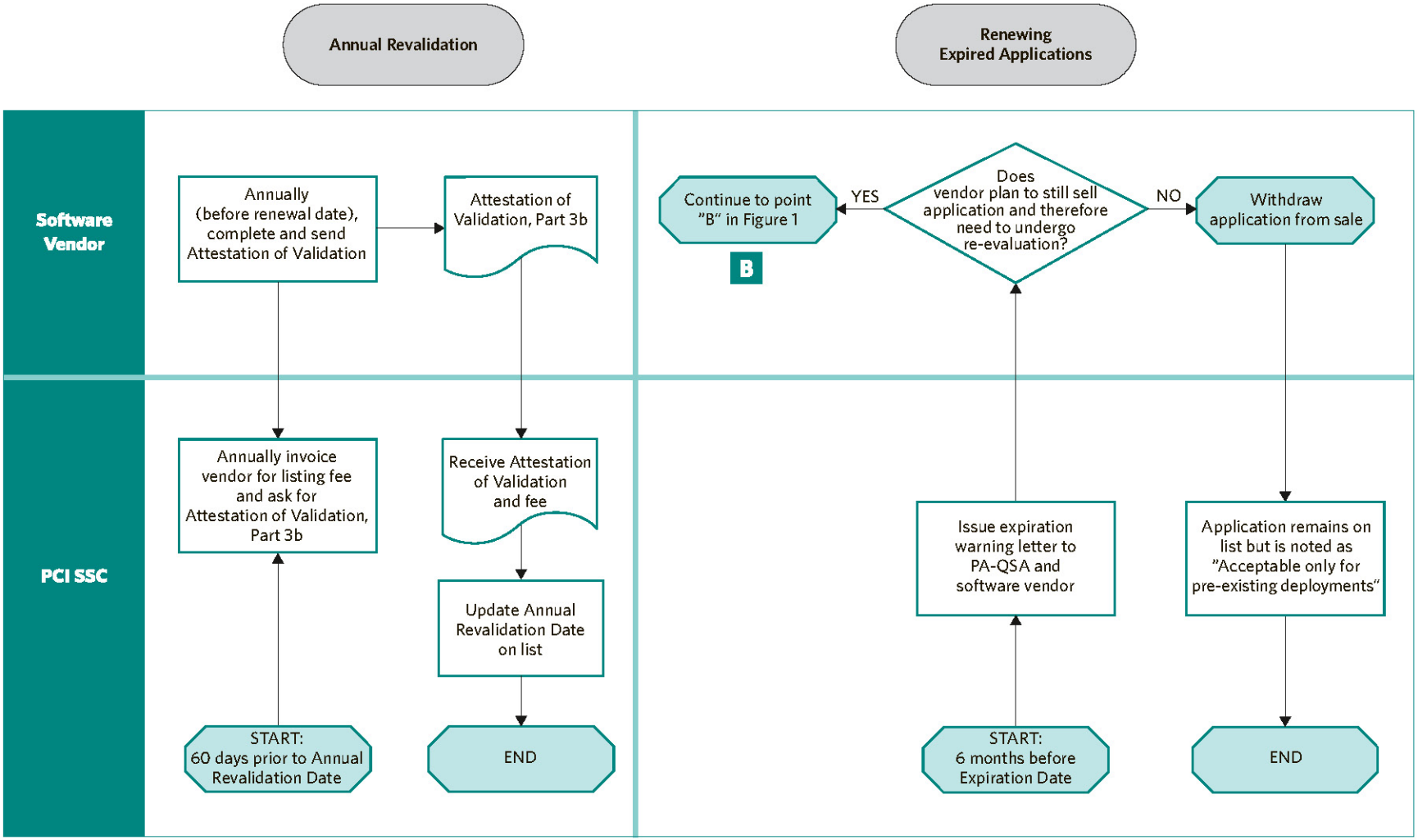
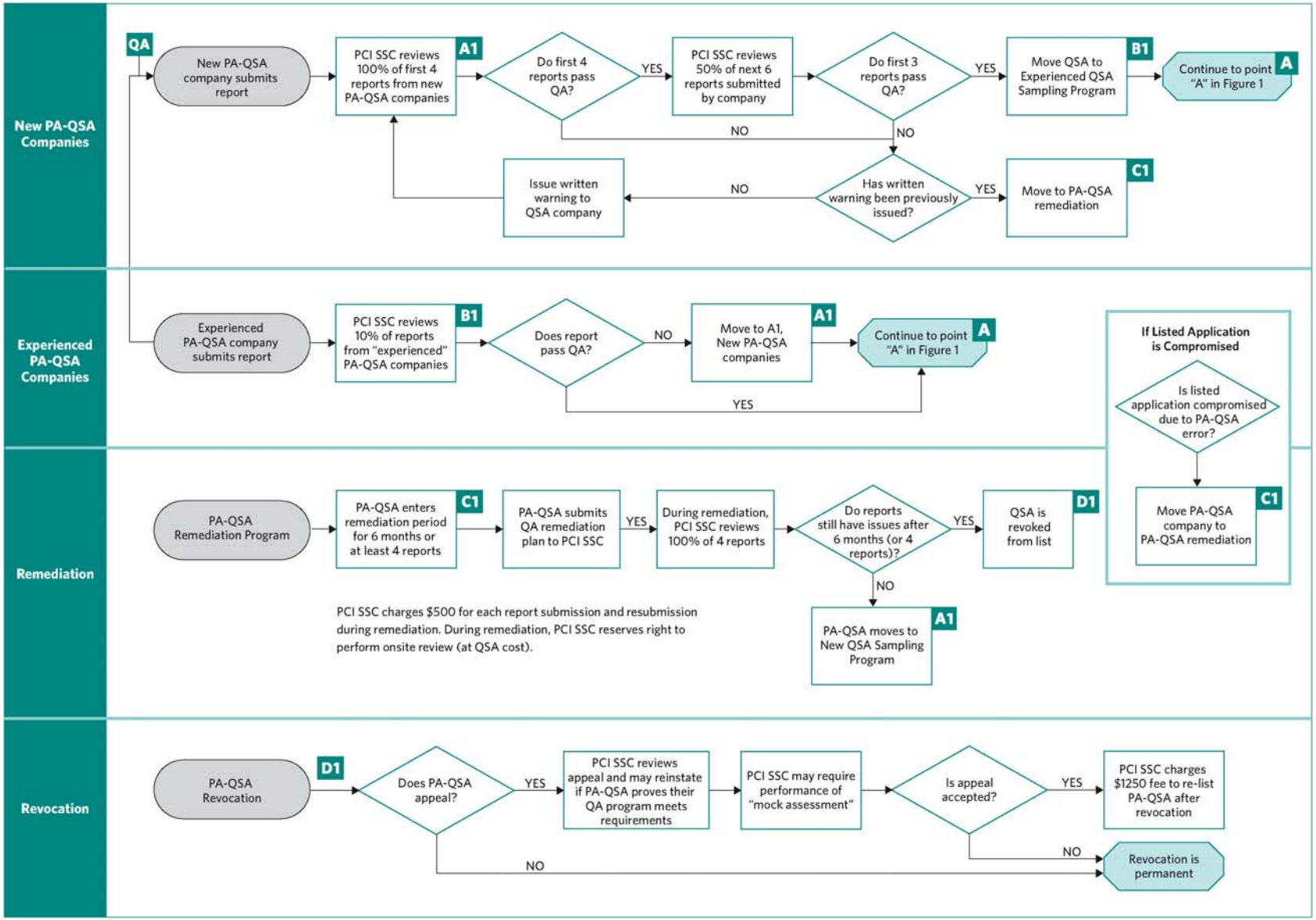


Figure 5: PA-QSA QA Programs for Report Reviews



PA-DSS Report Acceptance Process Overview

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

Note that all PA-DSS reports and other materials must be submitted to PCI SSC in English.

PCI SSC receives the report and reviews it from a quality assurance perspective. If the report meets the quality assurance requirements as documented in the QSA Validation Requirements and supporting documents, then PCI SSC sends a PA-DSS Acceptance Letter to the vendor and will add the application to the PCI SSC list by the end of the month for applications finalized by the 10th of that month. For quality issues associated with the report, PCI SSC communicates those issues with the PA-QSA. It is then the responsibility of the PA-QSA to resolve the issues with PCI SSC. The issues may be limited to updating the report to reflect adequate documentation to support the PA-QSAs decisions. However, if the issues require that the PA-QSA perform more testing, then the PA-QSA must notify the vendor that re- testing is needed and schedule that testing with the vendor.

The process flow for report acceptance is detailed in Figure 1.

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. Minor Update – No impact to PA-DSS requirements from minor changes made to a listed payment application. In this case, for the new version to be listed, the software vendor documents the change for the PA-QSA's review – see *Minor Update – No Impact on PA-DSS Requirements* section for specifics.
2. Major Update – Impact to PA-DSS requirements from changes made to a listed payment application. In this case, for the new version to be listed, the software vendor submits the new version of the payment application for a full PA-DSS review - see *Major Update - Impact on PA-DSS Requirements* section for specifics.
3. No Update – No changes made to a listed payment application. In this case, only an annual attestation section of the Attestation of Validation form is completed – see *No Changes to Listed Payment Application* section for specifics.

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, the vendor must submit the details of those changes to the PA-QSA, preferably to the PA-QSA that originally reviewed the payment application.

The PA-QSA then determines if a re-evaluation of the payment application is required. This decision is based on whether 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 *PA-DSS Acceptance Letter* and on the Website revised, the vendor must submit proper change documentation to the PA-QSA to determine whether a full evaluation needs to be performed. If the PA-QSA agrees with the vendor that the documented changes do not impact PA-DSS requirements, the PA-QSA will so communicate to the software vendor, the software vendor will prepare and sign a Self-Attestation of Minor Update, which the PA-QSA will also sign and then submit to PCI SSC. PCI SSC will then denote the updates accordingly in its revised *PA-DSS Acceptance Letter* and on the Website. See below under *Minor Update – No Impact on PA-DSS Requirements* for more information.

Note:

If payment application vendors can modularize the payment functionality, it would help minimize re-evaluations due to changes that do not impact payment functionality and security.

The process flow for changes to listed applications is detailed in Figure 2.

Minor Update – No Impact on PA-DSS Requirements

Change Analysis is Required

If a previously listed payment application is revised, but that revision is deemed to be minor and does not negatively impact security, then the software vendor prepares documentation of the change (a "Change Analysis") and submits the Change Analysis to the PA-QSA for review. It is strongly recommended that the vendor submits the Change Analysis to the same PA-QSA used for the original assessment.

The Change Analysis submitted by the software vendor to the PA-QSA should contain the following information at a minimum:

- Name of the payment application

- Payment application version number
- Related payment application name and version number currently on PCI SSC's list
- Description of the change
- 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 "minor" change
- If applicable, description of use of programming practices/module approaches and how such use prevents a negative impact to requirements.

If the PA-QSA agrees that the change as documented in the Change Analysis by the vendor does not negatively impact payment application security, (i) the PA-QSA will so notify the software vendor, (ii) the software vendor prepares and signs a Self-Attestation for Minor Update (Appendix C of this document), and sends it to the PA-QSA, (iii) the PA-QSA signs their concurrence and forwards it, along with the Change Analysis, to PCI SSC, and (iv) PCI SSC will then review the Self-Attestation and Change Analysis for quality assurance purposes.

Assuming no impact to PA-DSS requirements:

- A revised PA-DSS Acceptance Letter will be issued to the vendor.
- Upon payment of the minor update listing fees to PCI SSC as described in *Fees* above, the List of PA-DSS Validated Payment Applications on the Website would be updated accordingly with the new information. 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 with the Change Analysis, PCI SSC communicates those issues to the PA-QSA, and those issues are resolved according to the process described previously.

Major Update – Potential Impact on PA-DSS Requirements

New PA-DSS Review is Required

If changes to the payment application do impact PA-DSS requirements, the payment application must undergo another PA-DSS assessment. The PA-QSA will then submit a new PA-DSS report to the PCI SSC for acceptance. In this situation, the vendor may first submit documentation of the change to the PA-QSA, who will determine whether the nature of the change impacts payment application security in accordance with current PA-DSS requirements.

No Update – No Changes to Listed Payment Application

Annual Revalidation is Required

Annually, by the revalidation date noted on the list, the software vendor is required to submit an Attestation of Validation form with part 3b completed. The Attestation of Validation form is located in the *PA-DSS Requirements and Security Assessment Procedures, Appendix C*.

The process flow for annual revalidation is detailed in Figure 4.

Renewing Expired Applications

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

1. The vendor wants to continue to sell the application. If so, the vendor contacts a PA-QSA and has the payment application re-evaluated.
2. The vendor is not going to continue selling the application. If so, PCI SSC will change the listed status of the payment application to "acceptable only for **pre-existing** deployments"[2] after the expiration date. This provides assurance to those already using the payment application that the application is compliant.

Note that if the vendor chooses to continue selling the application, once the application successfully passes through the PA-DSS assessment process again, it retains its status on the PCI SSC List as "acceptable for new deployments"[3] and is assigned a new expiration date.

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

[2] "Acceptable only for **pre-existing** deployments – If a customer has already purchased and deployed this product, it is acceptable to continue using it. Note that the software vendor no longer sells and/or supports this product.

[3] "Acceptable for new deployments" – New customers may purchase and deploy this product.

Transition and Grandfathering of PABP-validated Payment Applications

Grandfathering PABP Applications on PABP List by October 15, 2008

PCI SSC is grandfathering (transferring) existing PABP-compliant applications onto the PCI SSC List. This grandfathering approach allows for applications that were previously evaluated and found compliant against PABP to continue being deployed until newer, PA-DSS-compliant, payment applications are available.

A phased approach has been applied to expiration dates of the PABP applications, dependent on the version of the requirements that were used to assess the application. In order to remain on the PCI SSC List as "acceptable for new deployments," the PABP-compliant applications need to be evaluated against the PA-DSS within prescribed timeframes. If a PABP-compliant application is not evaluated against the PA-DSS within prescribed timeframes, the application will remain on the PCI SSC List, but with the note "acceptable only for **pre-existing** deployments."

Note:

The PCI SSC List distinguishes between "new deployments" and "existing deployments." Payment applications often have a long lifetime once they are deployed, possibly up to 10-15 years. PCI SSC understands that the deployment of payment applications can be a complex and expensive process, and that it may not be practical for merchants and acquirers to update their payment applications every few years.

The following chart shows the respective expiration dates and notes that will be included on the *List of PA-DSS Validated Payment Applications* for the PABP versions as well as for PA-DSS reviews according to the current PA-DSS.

Version	Expiration Date	PCI SSC Listing Prior to Expiration		PCI SSC Listing After Expiration	
		Validation Notes	Deployment Notes	Validation Notes	Deployment Notes
PABP 1.4	24 months	Validated according to PABP	Acceptable for new deployments	Validated according to PABP	Acceptable only for **pre-existing** deployments
PABP 1.3	18 months	Validated according to PABP	Acceptable for new deployments	Validated according to PABP	Acceptable only for **pre-existing** deployments
Prior to PABP 1.3	12 months	Pre-PCI application	Not recommended for new deployments	Pre-PCI application	Acceptable only for **pre-existing** deployments
PA-DSS (any version)	3 years after change to standard	Validated according to PA-DSS	Acceptable for new deployments	Validated according to PA-DSS	Acceptable only for **pre-existing** deployments

The process flow for grandfathering and transitioning PABP applications is detailed in Figure 3.

Payment Applications Undergoing PABP Reviews during Transition

A grace period of approximately six months began on release of PA-DSS Version 1.1 in April 2008, allowing PA-QSAs to become familiar with the new standard, receive training, and become qualified to perform reviews against PA-DSS. Additionally, vendors could use this period to become familiar with PA-DSS and to address new PA-DSS requirements in developing their new payment applications.

During the grace period, payment applications could continue to be evaluated against PABP Version 1.4. The grace period was extended until **October 15, 2008**. Now that the grace period is over, reports based on PABP Version 1.4 not completed and accepted by October 15, 2008 are required to go through the *PA-DSS Transition Procedures*. The PA-QSA can submit the PABP report results, but must also include a delta evaluation according to the *PA-DSS Transition Procedures* in their submission to PCI SSC.

PA-DSS Transition Procedures

The PA-DSS Transition Procedures are to be used by Payment Application Qualified Security Assessors (PA-QSAs), where applicable, to bridge the gap between PABP and PA-DSS, for those applications for which a Visa PABP review was completed but not accepted by Visa prior to their due date of October 15, 2008.

***Note*:**

PCI SSC is "grandfathering" (or transferring) payment applications validated according to PABP Versions 1.3 and 1.4 to the List of PA-DSS Validated Applications *for 18 months and 24 months respectively, before a PA-DSS review will be required.*

These Transition Procedures are applicable in the following scenarios:

- ***Mandatory Completion of Transition Procedures:*** If a payment application is undergoing a PABP review that is not completed and accepted by Visa prior to October 15, 2008, then completion of these Transition Procedures is ***mandatory*** in order to have PCI SSC recognize these applications as validated according to PA-DSS. **Note that reviews done solely according to PABP will NOT be accepted after October 15, 2008**.
- ***Voluntary Completion of Transition Procedures:*** Per the *Note* above, if a payment application vendor has applications eligible for "grandfathering" but instead wants a PABP Version 1.3 or 1.4 application to be listed as "Validated according to PA-DSS," these Transition Procedures must be used. A PA-QSA would perform the procedures and submit the report according to the PA-DSS Program Guide in order for PCI SSC to recognize PABP Version 1.3 and 1.4 applications as validated.

Note:

The same PA-QSA company used to perform the PABP review should be used to perform the PA-DSS Transition Procedures.

For further information about the PA-DSS Transition Procedures, please refer to the *PABP to PA-DSS Transition Procedures* on the Website.

Note that PCI SSC will not accept PABP Transition Procedures after September 30, 2009*. After that time, PA-QSAs must submit only PA-DSS reports.*

Quality Assurance Program

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

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

New PA-QSA Sampling Program

A phased sampling process is used by PCI SSC to review ROVs from PA-QSAs – initially more reports are reviewed, and as the PA-QSA demonstrates quality the sampling rate is reduced. As the PA-QSA continues to meet quality standards, they pass into the Experienced QSA Sampling Program (with even lower sampling rates). As long as the PA-QSA meets quality standards, they will be subject to limited sampling.

However, if the PA-QSA does not meet the quality standards, the following actions are taken:

- Warning letter – provided to PA-QSA as an initial statement that the PA-QSA needs to improve quality.
- Remediation – if quality standards are still not being met, the PA-QSA is put into a remediation phase, and punitive actions may be initiated.
- Revocation – if quality standards are still not being met, the PA-QSA is revoked and removed from the PCI SSC list of approved PA-QSAs.

Experienced PA-QSA Sampling Program

Once a PA-QSA enters into the Experienced PA-QSA Sampling Program, limited sampling is performed on their reports. If quality standards continue to be met, then limited sampling continues. This is intended to be the “steady state” that PA-QSAs operate in.

If quality issues arise and standards are not met, then the PA-QSA falls back to the New PA-QSA Sampling Program.

Remediation

During remediation, PA-QSAs are still permitted to perform reviews, but all reports are QA reviewed by PCI SSC. PCI SSC will charge $500 each for all reports submitted and resubmitted during remediation.

The PA-QSA must also submit a remediation plan to PCI SSC detailing how the PA-QSA plans to improve quality of their reports. PCI SSC may also require an onsite visit with PA-QSA to audit their QA program, at the expense of the PA-QSA.

If the PA-QSA meets the quality standards during remediation, it moves back into the New PA-QSA Sampling Program. If the PA-QSA fails to meet quality standards during remediation, then the PA-QSA enters into Revocation.

Note that if a payment application included on the PCI SSC *List of PA-DSS Validated Payment Applications* is compromised due to PA-QSA error, then that PA-QSA will immediately be put under remediation. The PA-QSA will be required to meet the quality standards to move back into the New PA-QSA Sampling Program.

Revocation

When a PA-QSA is revoked, they are removed from the PCI SSC List of approved PA-QSAs. Once a PA-QSA is revoked, the PA-QSA cannot perform reviews of payment applications. The PA-QSA can appeal the revocation, but must meet requirements as documented in QSA Validation Requirements and supporting documents. PCI SSC reserves the right to require performance of a mock assessment.

Prior to re-entering the New PA-QSA Sampling Program, a re-listing fee of $1,250 will be assessed.

PA-DSS Reporting Processes

PCI SSC will base report acceptance solely on the results documented in the ROV. Upon receipt of the report, the following will apply:

- PCI SSC shall review the report (generally within thirty calendar days of receipt) and determine if it is acceptable
- If no issues or questions to the PA-QSA are identified, PCI SSC shall bill the software vendor for the listing fee. Once the listing fee is received, PCI SSC will issue a PA-DSS Acceptance Letter and post the payment application and vendor's information to the Website
- If questions or issues are identified and sent to the PA-QSA, the process described above will restart upon receipt of a complete and acceptable revised report or response ("Revised Report") from the PA-QSA. The process re-start does not occur until receipt of an acceptable Revised Report addressing all previously identified items. PCI SSC will generally review a Revised Report within 30 calendar days of receipt.
- Should additional questions or issues arise, the cycle repeats until a satisfactory response is received, at which time PCI SSC will issue the PA-DSS Acceptance Letter and post the information to the Website. Additional issues or questions may be raised at any time prior to issuance of a PA-DSS Acceptance Letter.

For reports related to minor updates to existing listed application versions, based on vendors' Self-Attestation of Change, the above PA-DSS Report Acceptance process is the same, and PCI SSC shall issue a revised PA-DSS Acceptance Letter and post the revised information to the Website unless issues or questions arise, in a manner similar to the aforementioned.

The PCI SSC acceptance letter and listing on the Website will contain, at minimum, the information listed below. Each characteristic is detailed in "*Appendix A: Application Elements for 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
  - Self-Attestation for Minor Update, if applicable
  - Description Provided by Vendor
  - Components Included in Review
- Validated According to (PABP or PA-DSS version)
- Deployment Notes
- Revalidation Date
- Expiry Date
- PA-QSA Company
- Specific Region or Locale for Payment Application, if applicable

***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.

Notification Following a Security Breach, Compromise, or Known Vulnerability

Vendors must notify PCI SSC of any security breach or compromise that occurs in relation to a listed payment application, or if the vendor becomes aware of a vulnerability in the payment application, using the procedures described in this section.

Notification and Timing

Notwithstanding any other legal obligations the vendor may have, the vendor must immediately notify PCI SSC of any security breach, compromise, or known vulnerability relating to any vendor's payment application listed by PCI SSC.

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

Note:

Notification must take place no later than 24 hours after the vendor first discovers the security breach or compromise.

Notification Format

The vendor's initial notification of a security breach, compromise, or known vulnerability must take the form of a phone call to the PCI SSC PA-DSS Coordinator, followed by an e-mail, fax, or letter providing full details of the security breach or compromise.

Notification Details

Following notification of a security breach, compromise, or known vulnerability, the vendor must supply the PCI SSC PA-DSS Coordinator with all relevant information relating to the issue. This will include, but is not limited to:

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

PCI SSC, as agreed within the terms of the Vendor Release Agreement, may share this information and other information as required to support or enable an evaluation of the security breach, compromise, or vulnerability to be performed to mitigate or prevent further security breaches or compromises.

Actions following a Security Breach or Compromise

In the event of PCI SSC's being made aware of a security weakness or actual compromise related to a specific product, or group of products, as listed in the *List of PA-DSS Validated Payment Applications*, PCI SSC may take the following actions:

- Notify all payment brands that a security weakness or compromise has occurred.
- Attempt to obtain the forensics report to evaluate exactly how the compromise occurred.
- Contact the vendor to inform them that their product has a security weakness, or has been compromised and, where possible, share information relating to the actual weakness or compromise.
- Support the vendor's efforts to try and mitigate or prevent further compromises.
- Support the vendor's efforts to 1) correct any security weaknesses, and 2) produce a guideline document to be issued to that vendor's customers, informing them of any potential vulnerability and

detailing what actions should be taken in order to mitigate or prevent further security breaches or compromises.

- Work with appropriate law enforcement agencies to help mitigate or prevent further compromises.
- Support and/or enable evaluations on the compromised product either internally or under the terms of the Release Agreement, using PA-QSAs to identify the cause of the compromise.

Withdrawal of Acceptance

PCI SSC reserves the right to withdraw a payment application's acceptance and remove that payment application from the *List of PA-DSS Validated Payment Applications*, when it is clear that the payment application does not offer sufficient protection against current threats and/or does not conform to PA-DSS requirements. If PCI SSC considers that the payment application has a security weakness or has been compromised, PCI SSC will notify the vendor in writing of its intent to withdraw its acceptance of that payment application.

Legal Terms and Conditions

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

No vendor or other third party may refer to a payment application as "PCI Approved," or "PCI SSC Approved" nor otherwise state or imply that PCI SSC has, in whole or part, approved any aspect of a vendor or its payment applications, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with PCI SSC, or in a PA-DSS letter of acceptance provided by PCI SSC. All other references to PCI SSC's acceptance of a payment application or version thereof are strictly and actively prohibited by PCI SSC.

When granted, PCI SSC acceptance is provided to ensure certain security and operational characteristics important to the achievement of PCI SSC's goals, but such acceptance does not under any circumstances include or imply any endorsement or warranty 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 noninfringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services that have received acceptance from PCI SSC, shall be provided by the party providing such products or services, and not by PCI SSC or any payment brands.

.

Appendix A: Elements for Acceptance Letter and *List of Validated Payment Applications*

Payment Application Vendor

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

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
- Self-Attestation for Minor Update, if applicable
- Description Provided by Vendor
- Components Included in Review

Example of a Payment Application Identifier:

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

Payment Application Identifier: Detail

- **Payment Application Name**

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

- **Payment Application Version #**

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

  Note:

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

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

- **Payment Application Type**

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

Type	Function	Description
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.
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.
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.
08	POS Face-to-Face	Point of sale software used by merchants solely for face-to-face payment card transactions. These applications may or may include middleware, front office or back office software, store management software, etc.
01	POS Suite	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.
06	POS Specialized	Point of sale software which can be used by merchants for specialized transmission methods, such as Bluetooth, mobile, cell phone, 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.
09	Shopping Cart & Store Front	Payment software for eCommerce 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.

- **Target Market, if applicable**

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

  - Retail
  - Processors
  - Gas/oil
  - e-Commerce
  - Small/medium merchants

  Note:

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

- **Reference Number**

  PCI SSC assigns the Reference number at the time of acceptance; 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)

- **Self-Attestation for Minor Update, if applicable**

  Self-Attestation for Minor Update is used where applicable, to denote those application versions that undergo the process documented in the "Minor Updates – No Impact on PA-DSS Requirements" section of this document.

- **Description Provided by Vendor**

- **Components Included in Review**

  This section for Components Included in Review is to include reviewed software components that only operate with the listed payment application. Components included here will not function without the listed payment application and are never individually sold.

Validated According To

"Validated According To" is used by PCI SSC to denote whether the review was according to Visa's PABP program or PCI SSC's PA-DSS program, and to note the applicable version of PABP or PA-DSS. Please see table under Deployment Notes below for examples.

Deployment Notes

Deployment Notes are used by PCI SSC to denote one whether a payment application is acceptable or acceptable only for **pre-existing** deployments, and is related to the payment application's Expiration Date, noted below. Please also refer to the full table on page 24 for more details.

PCI SSC Listing prior to expiration		PCI SSC Listing after expiration	
Validation Notes	**Deployment Notes**	**Validation Notes**	**Deployment Notes**
Validated according to PABP	Acceptable for new deployments	Validated according to PABP	Acceptable only for **pre-existing** deployments
Pre-PCI application	Not recommended for new deployments	Pre-PCI application	Acceptable only for **pre-existing** deployments
Validated according to PA-DSS	Acceptable for new deployments	Validated according to PA-DSS	Acceptable only for **pre-existing** deployments

Revalidation Date

The **Revalidation Date** is used by PCI SSC to indicate when the software vendor's annual Attestation of Validation is due. The Annual Revalidation is part of the Attestation of Validation form, located in PA-DSS Appendix C, part 3b.

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 24-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.

Note:

Any PA-DSS assessments done against Version 1.1 will receive the same expiration date as reviews done against PA-DSS Version 1.2, in accordance with the normal expiration process.

For example: PA-DSS Version 1.1 and Version 1.2 will have the same expiration date. With the next PA-DSS version (the one following Version 1.2) expected in approximately October 2010, reviews against PA-DSS Versions 1.1 and 1.2 will expire in October 2013.

There is currently no sunset date for PA-DSS validated payment applications that were on the list 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.

PA-QSA Company

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

Specific Region or Locale, if applicable

The Specific Region or Locale for Payment Application denotes payment applications that are developed for, and can only be used in, specific geographic regions or locales.

Appendix B: Identification of Certified Payment Application Builds

Note: *For future consideration.*

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

For example, such a method could include the following:

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

Appendix C: Self-Attestation for Minor Update

Instructions for Submission

The Payment Application Vendor and Payment Application Qualified Security Assessor (PA-QSA) must complete this document as a declaration of the payment application's change status with the Payment Application Data Security Standard (PA-DSS). The Payment Application Vendor should complete all applicable sections and submit the Change Analysis document and this Self-Attestation to the PA-QSA.

Subsequent to review of the supplied documentation, the PA-QSA should complete the applicable sections and submit along with copies of all required documentation to PCI SSC at using PCI SSC's instructions for report encryption and submission.

Part 1. Payment Application Vendor Information					
Company Name:					
Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP:	
URL:					

Part 1a. Payment Application Information		
"Parent" Payment Application Name and Version Number currently on the PCI SSC list:		
Existing Application Name:	Existing Version Number:	
PCI SSC Approval Number:		
New Payment Application Name and Version Number, if applicable:		
New Application Name:	New Version Number:	
Description of change, if applicable:		
Payment Application Functionality (check all that apply):		
☐ POS Suite	☐ POS Admin	☐ Shopping Cart & Store Front
☐ POS Face-to-Face	☐ Payment Middleware	☐ Others (please specify):
☐ POS Kiosk	☐ Payment Back Office	
☐ POS Specialized	☐ Payment Gateway/Switch	
Target Market for Application:		

Part 2. Payment Application Qualified Security Assessor (PA-QSA) Company Information

Company Name:					
Lead PA-QSA Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP:	
URL:					

Part 3. Confirmation of Change Status

Part 3a. Payment Application Vendor Attestation

Based on internal change analysis and Change Analysis documentation, *(PA Vendor Name)* asserts the following status for the application(s) and version(s) identified in Part 1a of this document as of *(date)* (check applicable fields):

☐	*Only minor changes* have been made to the "Parent" application noted above to create the New application also noted above, resulting in **No Impact** to the PA-DSS requirements.
☐	All changes have been accurately recorded in the accompanying Change Analysis document provided to the PA-QSA noted in Part 2.
☐	All information contained within this self-attestation represents the results of the change analysis fairly in all material respects.
☐	There is no evidence of magnetic stripe (i.e., track) data[3], CAV2, CVC2, CID, or CVV2 data[4], or PIN data[5] storage subsequent to transaction authorization on ANY files or functionalities generated by the application.

Part 3b. Payment Application Qualified Security Assessor (PA QSA) Attestation

Based on the Change Analysis documentation provided by the Payment Application Vendor noted in Part 1, *(PA-QSA Name)* asserts the following status for the application(s) and version(s) identified in Part 1a of this document as of *(date)* (check applicable fields):

☐	Based on our review of the Change Analysis documentation, we agree that the documentation supports the vendor's assertion that *only minor changes* have been made to the application noted above, resulting in **No Impact** to the PA-DSS requirements

[3] Magnetic Stripe Data (Track Data) – Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic stripe data after authorization. The only elements of track data that may be retained are account number, expiration date, and name.

[4] The three- or four-digit value printed on the signature panel or face of a payment card used to verify card-not-present transactions.

[5] PIN Data – Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 3c. PA-QSA and Application Vendor Acknowledgments

Signature of Lead PA-QSA ↑	*Date* ↑
Lead PA-QSA Name ↑	*Title* ↑
Signature of Application Vendor Executive Officer ↑	*Date* ↑
Application Vendor Executive Officer Name ↑	*Title* ↑
Application Vendor Company Represented ↑	