Payment Card Industry (PCI)

Software Security Framework
Secure Software Standard

Program Guide

Version 1.0.1

July 2020

Document Changes

Date	Version	Description
June 1, 2019	1.0	Initial release
July 2020	1.0.1	Aligned language (regarding use of wildcards) in Appendix B "Payments Software Versioning Methodology" and section 3.1 "Vendors" with language in the *Secure Software Report on Validation (ROV)* report template.

Contents

1 Introduction

This Program Guide provides information for vendors of payment software ("Payment Software") wishing to participate in the Payment Card Industry ("PCI") Secure Software Standard program operated by PCI SSC ("Secure Software Program" or "Program"), and for companies that are qualified to perform assessments against the PCI Secure Software Standard for Program purposes (each such assessment, for purposes of this Program Guide, a "Secure Software Assessment" or "Assessment").

The PCI Secure Software Standard is part of the PCI Software Security Framework ("SSF"). This Program Guide details information pertinent to the roles of SSF Assessor Companies authorized by PCI SSC to perform Secure Software Assessments under the Program ("Secure Software Assessor Companies" or "Assessors"), and their employees who are qualified by PCI SSC to perform such Assessments ("Secure Software Assessor-Employees").

Companies and individuals wishing to become qualified by PCI SSC to perform Secure Software Assessments should first consult the *Payment Card Industry (PCI) Software Security Framework Qualification Requirements for Assessors* on the Website (the "SSF Qualification Requirements").

Capitalized terms used but not otherwise defined herein have the meanings set forth in the SSF Qualification Requirements, as applicable.

2 Related Publications

This Program Guide should be used in conjunction with other relevant PCI SSC publications, including but not limited to current publicly available versions of the following, each available on the PCI SSC web site ("Website"):

Document name	Description
Payment Card Industry (PCI) Secure Software Standard ("PCI Secure Software Standard")	Defines a baseline set of specific technical requirements and assessment procedures against which Payment Software must be successfully validated to be qualified by PCI SSC as Validated Payment Software (See Sections 2.1 and 4 below).
Payment Card Industry (PCI) Software Security Framework Secure Software Lifecycle Requirements and Assessment Procedures ("PCI Secure SLC Standard")	Defines a baseline set of specific technical requirements and assessment procedures against which vendors must be successfully assessed to be qualified by PCI SSC as Secure SLC Qualified Vendors.
Payment Card Industry (PCI) Software Security Framework Glossary of Terms, Abbreviations, and Acronyms	A glossary of terms used within the Software Security Framework.
Payment Card Industry (PCI) Report on Validation Reporting Template for Secure Software Standard ("ROV Report Template")	The template document provided by PCI SSC and required to be used by Assessors to prepare PCI Secure Software Standard Reports on Validation ("ROVs"). The ROV Report Template includes details on how to document the findings of a Secure Software Assessment.
Secure Software Attestation of Validation	A template document provided by PCI SSC and required to be used by Secure Software Assessor Companies and Vendors to attest to the results of Secure Software Assessments.
Payment Card Industry (PCI) Software Security Framework Qualification Requirements for Assessors ("SSF Qualification Requirements")	Defines the baseline set of requirements that must be met by SSF Assessor Companies and their Assessor-Employees to perform Secure Software Assessments or Secure SLC Assessments.
Vendor Release Agreement ("VRA")	Establishes the terms and conditions under which Vendors of Validated Payment Software participate in the Program.
PCI SSC Programs Fee Schedule	Lists the current fees for specific qualifications, tests, retests, training, and other services.
Secure Software Assessor Feedback Form	Template document made available by PCI SSC and required to be provided by Secure Software Assessors to their vendor customers to solicit feedback regarding such Secure Software Assessors and their Secure Software Assessment process.

2.1 PCI Secure Software Standard

The PCI Secure Software Standard details the requirements that Payment Software must meet in order to be validated against the PCI Secure Software Standard and qualified by PCI SSC for Program purposes ("Validated Payment Software" or "Listed" Payment Software). Validation helps assure that Payment Software is developed with security to protect the integrity of the software and the confidentiality of sensitive data it captures, stores, processes, and transmits. Validated Payment Software is identified on PCI SSC's list of Validated Payment Software on the Website (the "List of Validated Payment Software").

2.2 Relationship between PCI Secure Software Standard and other PCI SSC Standards

The PCI Secure Software Standard is separate and independent from other PCI SSC standards. The use of Validated Payment Software may help support the security of an entity's cardholder data environment, but does not make an entity PCI DSS compliant, or imply compliance with or result in validation to any other PCI SSC standard. Entities must ensure that all Payment Software is implemented in a PCI DSS compliant manner and included in their PCI DSS assessment to verify the software is properly configured and meets applicable PCI DSS requirements.

2.3 Relationship between PCI Secure Software Program and PCI Secure SLC Program

Payment Software that is successfully assessed and validated under a Software Security Assessor Company using the Secure Software Program has been determined, by the applicable Secure Software Assessor Company, to be in compliance with the PCI Secure Software Standard.

Vendors that are successfully validated under the PCI Secure SLC Standard Program ("Secure SLC Qualified Vendors") to have demonstrated to the applicable Secure SLC Assessor Company that their validated secure payment software development life cycle processes, procedures, and practices are in compliance with the PCI Secure SLC Standard. Secure SLC Qualified Vendors are:

- Identified on PCI SSC's list of Secure SLC Qualified Vendors on the Website; and
- Authorized to perform certain types of "Delta" assessments (See Section 4.1 below) of their own Validated Payment Software under the Program with reduced Secure SLC Assessor participation, where the Payment Software (a) is Validated Payment Software and (b) was developed and managed under processes that are identified for that Vendor on PCI SSC's list of Secure SLC Qualified Vendors.

***Note**: Vendors of Validated Payment Software are not required to be Secure SLC Qualified Vendors in order to submit their Payment Software for Secure Software Assessment.*

2.4 Updates to Documents and Standards

This Program Guide is expected to change as necessary to align with updates to the PCI Secure Software Standard and other related PCI SSC publications. Additionally, PCI SSC provides interim updates to the PCI community through a variety of means, including (without limitation) required assessor training, e-mail bulletins and newsletters, and frequently asked questions.

PCI SSC reserves the right to add, change, or withdraw any security, qualification, training, and/or other requirements at any time.

3 Roles and Responsibilities

There are several stakeholders involved in the Secure Software Program. The following sections describe their respective roles and responsibilities in connection with Program participation.

3.1 Vendors

Vendors are responsible for:

- Creating PCI Secure Software Standard compliant Payment Software;
- Ensuring they, and the Payment Software products they submit for validation under the Program, satisfy all applicable requirements of the PCI Secure Software Standard (and modules thereof) and Program (collectively, "Secure Software Requirements"), including but not limited to successfully passing a Secure Software Assessment as specified in *PCI Secure Software Requirements and Validation Procedures;*
- Complying with the *Vendor Release Agreement* including the adoption and implementation of Vulnerability Handling Policies (defined in the VRA) consistent with industry best practices;
- Creating security guidance (as required by Control Objective 12, "Vendor Security Guidance" in the PCI Secure Software Standard) for each Payment Software product submitted for validation under the Program (*"Security Guidance"*). In addition to general instruction, the *Security Guidance* must specifically detail the steps required to ensure the secure implementation, configuration, and operation of the applicable Payment Software in accordance with the requirements of the *PCI Secure Software Standard;*
- Providing their customers (directly or indirectly through their integrators and resellers) with a copy of the applicable *Security Guidance*. This includes applicable mapping of internally used version numbers to those that have been published on the Website, and any subsequent updates to the *Security Guidance* that may result from changes to the Validated Payment Software over time;
- Submitting their Payment Software products and supporting documentation to the Secure Software Assessor Company for review and authorizing their Secure Software Assessor Company to submit resulting Reports on Validation (ROVs) and related information to PCI SSC;
- Paying all invoices from PCI SSC in a timely fashion; and
- Staying up to date with PCI Secure Software Standard, Secure Software Program documents, statements and guidance on the Website, as well as industry trends and best practices.

3.2 Payment Card Brands

The Payment Card Brands develop and enforce their own programs related to PCI Secure Software Standard compliance, including, but not limited to:

3.3 PCI Security Standards Council

PCI SSC is the standards body that maintains the PCI SSC standards. In relation to Secure Software Program, PCI SSC:

- Maintains a centralized repository for all Reports on Validation (ROVs) for Validated Payment Software listed on the Website;
- Hosts the List of Validated Payment Software on the Website;

- Provides training for and qualifies Secure Software Assessor Companies and Secure Software Assessor Employees to perform Secure Software Assessments.
- Lists Secure Software Assessor Companies on the Website.
- Maintains and updates the PCI Secure Software Standard and related documentation according to a standards lifecycle management process; and
- Reviews all ROVs and related change submissions to confirm that:
  - Submissions (including ROVs, updates and Annual Revalidations) are correct as to form;
  - Secure Software Assessor Companies properly determine whether candidate Payment Software is eligible for validation under the Secure Software Program; and
  - Detail provided in such submissions (ROVs, updates, and Annual Revalidations) meets PCI SSC's reporting requirements.

***Note**: PCI SSC reserves the right to reject or delist any Payment Software determined to be ineligible for the Secure Software Program.*

As part of the quality assurance ("QA") process for the Program, Secure Software Assessor Companies must demonstrate to PCI SSC that they meet PCI SSC's QA and Program qualification requirements, and PCI SSC assesses whether Secure Software Assessor Company operations appear to conform to PCI SSC's QA and Program qualification requirements.

***Note**: PCI SSC does not perform Assessments of or validate Payment Software for compliance with the PCI Secure Software Standard; Assessment and validation are the roles of the Secure Software Assessor Company and its Secure Software Assessor Employees. Listing of Payment Software on the List of Validated Payment Software signifies that the applicable Secure Software Assessor Company has determined that the applicable Payment Software complies with the PCI Secure Software Standard, that the Secure Software Assessor Company has submitted a corresponding ROV to PCI SSC, and that PCI SSC has determined that such ROV has satisfied all PCI SSC documentation requirements for ROVs as of the time of PCI SSC's review.*

3.4 Secure Software Assessor Companies

Secure Software Assessor Companies (with at least one Secure Software Assessor-Employee at all times) are qualified by PCI SSC to perform Secure Software Assessments, subject to continued compliance with Program requirements. Secure Software Assessor Companies are responsible for:

- Performing Secure Software Assessments in accordance with the PCI Secure Software Standard, this Program Guide, the SSF Qualification Requirements, and the SSF Agreement;
- Providing an opinion in the applicable ROV regarding whether the Payment Software meets the intent and requirements of PCI Secure Software Standard;
- Documenting each Secure Software Assessment in a ROV using the ROV Report Template;
- Providing adequate documentation within the ROV to demonstrate the Payment Software's compliance with the PCI Secure Software Standard;
- Submitting each ROV and/or any change submissions to PCI SSC, along with the completed *Secure Software Attestation of Validation ("AOV")*, each signed by the Secure Software Assessor Company and Vendor, and the Vendor's executed VRA, if applicable;
- Maintaining an internal quality assurance process for their Secure Software Assessment efforts;
- Staying up to date with PCI SSC statements and guidance, industry trends, and best practices;

- Satisfying all applicable SSF and Program requirements at all times, including but not limited to the successful completion of annual revalidation, adhering to the applicable SSF Qualification Requirements, and ensuring that Secure Software Assessor-Employees have completed all required training and training examinations.

It is the Secure Software Assessor Company's responsibility to assess a Vendor's Payment Software for compliance with the PCI Secure Software Standard as of the date of the Secure Software Assessment and document its findings and opinions on compliance in the applicable ROV using the ROV Report Template. PCI SSC does not approve ROVs from a technical compliance perspective; it performs quality assurance to confirm that the ROVs adequately document the Secure Software Assessor Company's validation and attestation of compliance.

3.5 Customers

Customers are merchants, service providers, or others who buy or receive third-party Payment Software products. Customers seeking Validated Payment Software are responsible for:

- Selecting Validated Payment Software from the Website and ensuring that the Payment Software's version information is consistent with that indicated on the Website;
- Implementing such software within a PCI DSS compliant environment;
- Configuring the Payment Software (where configuration options are provided) according to the associated *Security Guidance* provided by the Vendor;
- Configuring such Payment Software in a PCI DSS compliant manner; and
- Maintaining the PCI DSS compliant status of both the environment and the Payment Software's configuration.

Customers and others can find the List of Validated Payment Software on the Website along with other reference materials. PCI SSC's List of Validated Payment Software is the authoritative listing of Validated Payment Software.

4 Overview of Validation Processes

4.1 Secure Software Assessments

There are two types of Secure Software Assessments under the PCI Secure Software Standard:

- Full Software Assessments
- Interim or "Delta" Assessments

All software submitted for Secure Software Assessment must be validated against both:

- The Core Requirements of the PCI Secure Software Standard; and
- EACH module of the PCI Secure Software Standard that applies to that type of software.

***Note**: Additional modules for the PCI Secure Software Standard are expected to be added to the standard in the future.*

4.1.1 Full Software Assessments

Full Software Assessments involve a detailed technical analysis of the entire scope of the Payment Software and are intended to independently validate that the software meets all applicable requirements of the PCI Secure Software Standard. Full Software Assessments are performed by a PCI-qualified Secure Software Assessor Employee of a Secure Software Assessor Company. See Section 6.2 "Changes to Listed Payment Software ," for more information.

***Note**: Validation of a software product is not dependent on the software vendor being Secure SLC Qualified unless otherwise directed by a payment brand.*

4.1.2 Delta Assessments

Delta Assessments are required upon changes to Validated Payment Software that occur between Full Software Assessments. Delta Assessments confirm that software updates do not introduce new vulnerabilities and the software continues to meet applicable Secure Software Requirements. Additional details regarding the Delta Assessment process can be found in Section 6.2, "Changes to Listed Payment Software."

4.2 Initial Validation and Listing

The following is a high-level overview of the process for initiating and completing a Secure Software Assessment:

- The Vendor initiates the process by selecting a Secure Software Assessor Company from the Website and negotiates any costs and agreements necessary for the Secure Software Assessor Company to perform the Assessment with the Secure Software Assessor Company.
- The Vendor and the Secure Software Assessor Company determine the scope of the Assessment, including identifying all Program requirements and applicable materials necessary to perform the Assessment in accordance with Secure Software Program requirements.
- The Secure Software Assessor Company assesses the Payment Software, including its security functions and features, to determine whether the software complies with all applicable requirements of the *PCI Secure Software Standard*.

- If the Secure Software Assessor Company determines that the Vendor's Payment Software satisfies all applicable requirements, it prepares a corresponding Report on Validation (ROV) including all test results, opinions, and conclusions of the Secure Software Assessor Company, along with a completed Secure Software Attestation of Validation (AOV), and submits them to PCI SSC for review.
- The Vendor pays all invoices from PCI SSC in a timely fashion.
- PCI SSC reviews the submission (including the ROV), all test results, Vendor evidence, Assessor opinions, and conclusions to determine that the submission demonstrates reasonable assurance that testing was performed satisfactorily and that the requirements have been met.
- Upon and subject to successful completion of the submission review process and final acceptance and approval of the ROV by PCI SSC ("Acceptance"), PCI SSC will add a listing identifying the assessed Payment Software to its List of Validated Payment Software on the PCI SSC website. Validated Payment Software listings are generally valid for a period of up to three years (subject to delisting and expiration in accordance with the VRA and Program requirements and rules).

The illustrations and descriptions on the following pages explain in further detail the elements of the Secure Software Program:

Process	Illustration	Page	Related Section
PCI Secure Software Standard Initial Validation and Listing Process	Figure 1	9	Section 4.2
PCI Secure Software Standard Annual Attestation and Renewing Expiring Software	Figure 2	10	Section 6.1 & 6.2.3
Changes to Listed Payment Software	Figure 3a & 3b	11 & 12	Section 6.2

Figure 1: Secure Software Standard Initial Validation and Listing Process

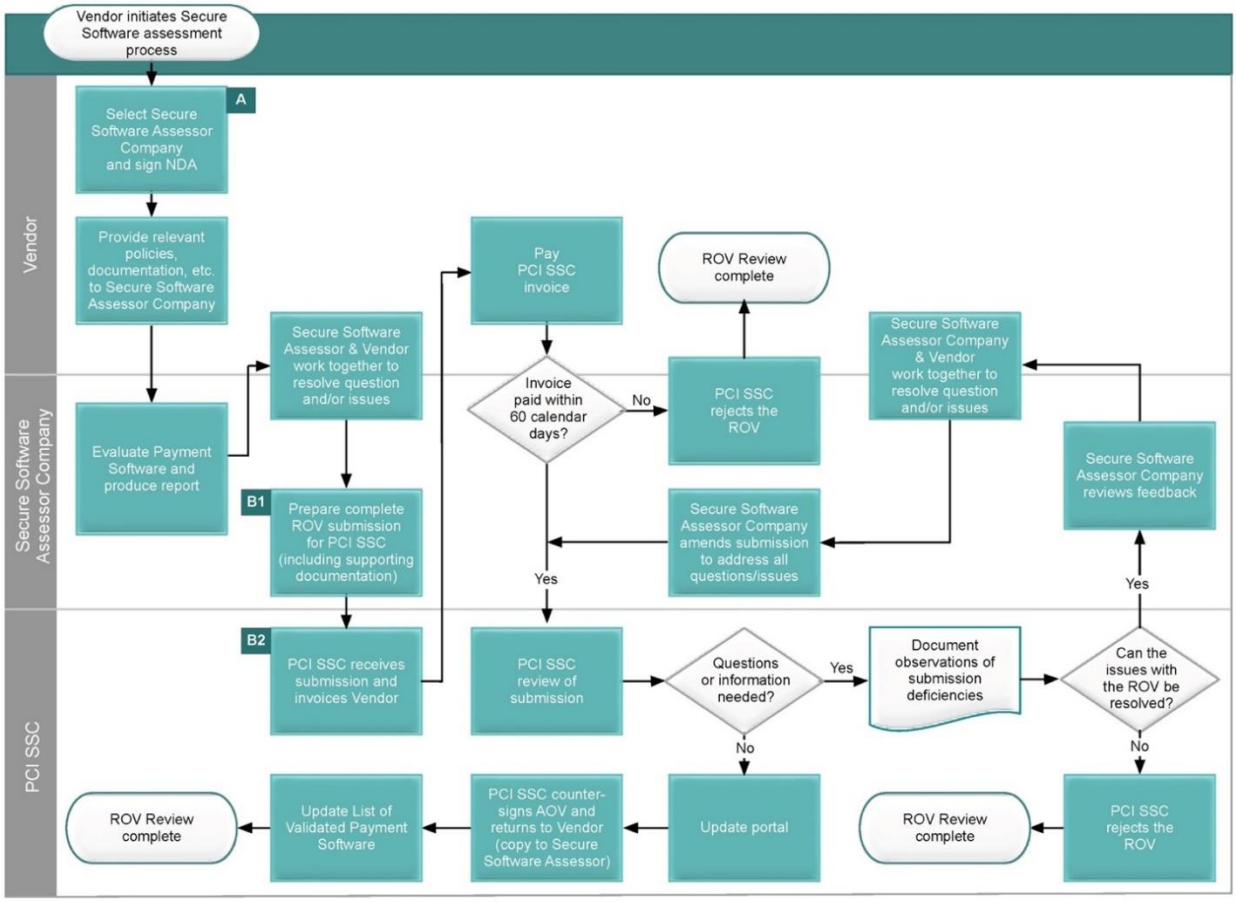


Figure 2: Secure Software Standard Annual Attestation and Renewing Expiring Software

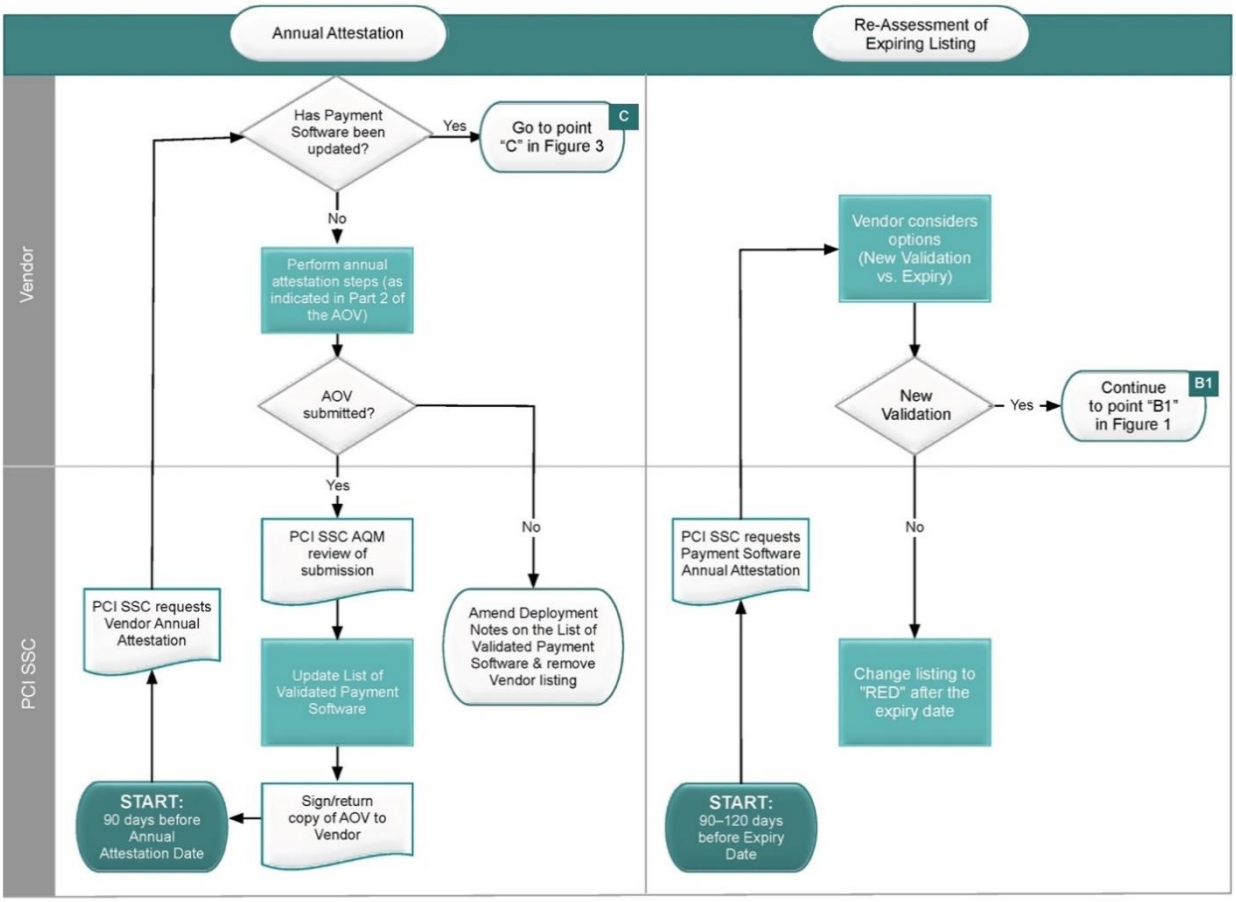


Figure 3a: Updates to Listed Payment Software – Not a Secure SLC Qualified Vendor

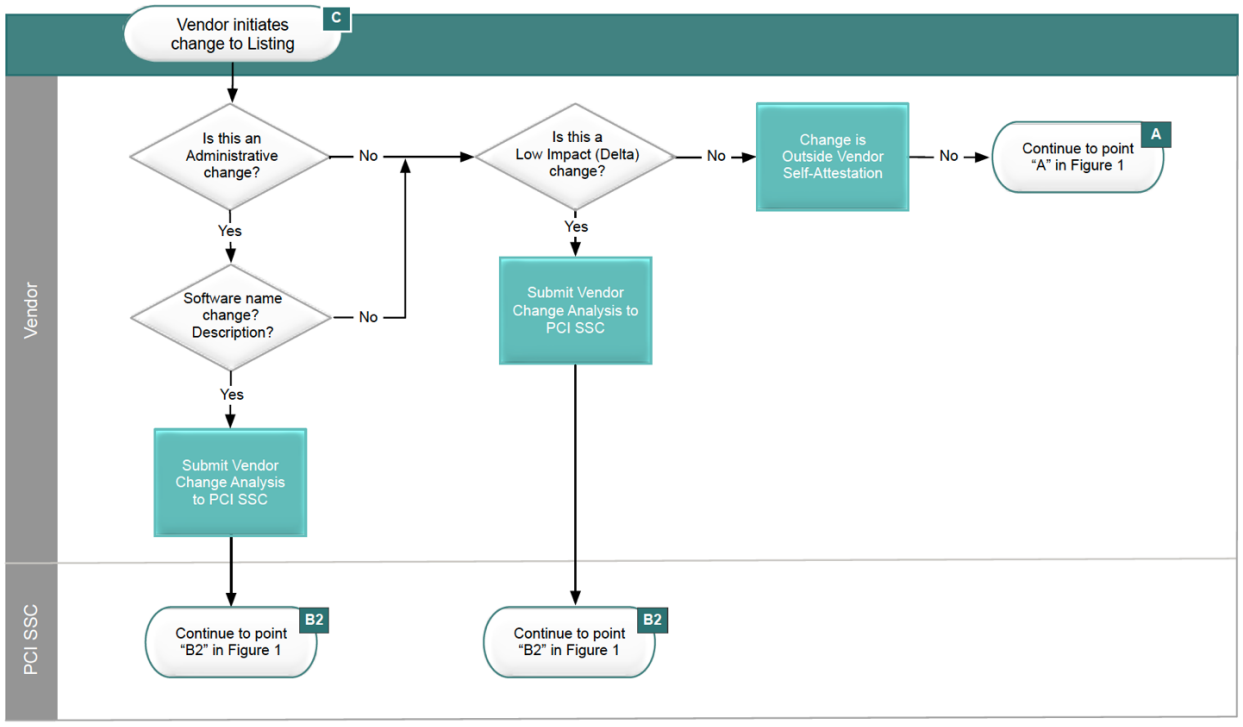
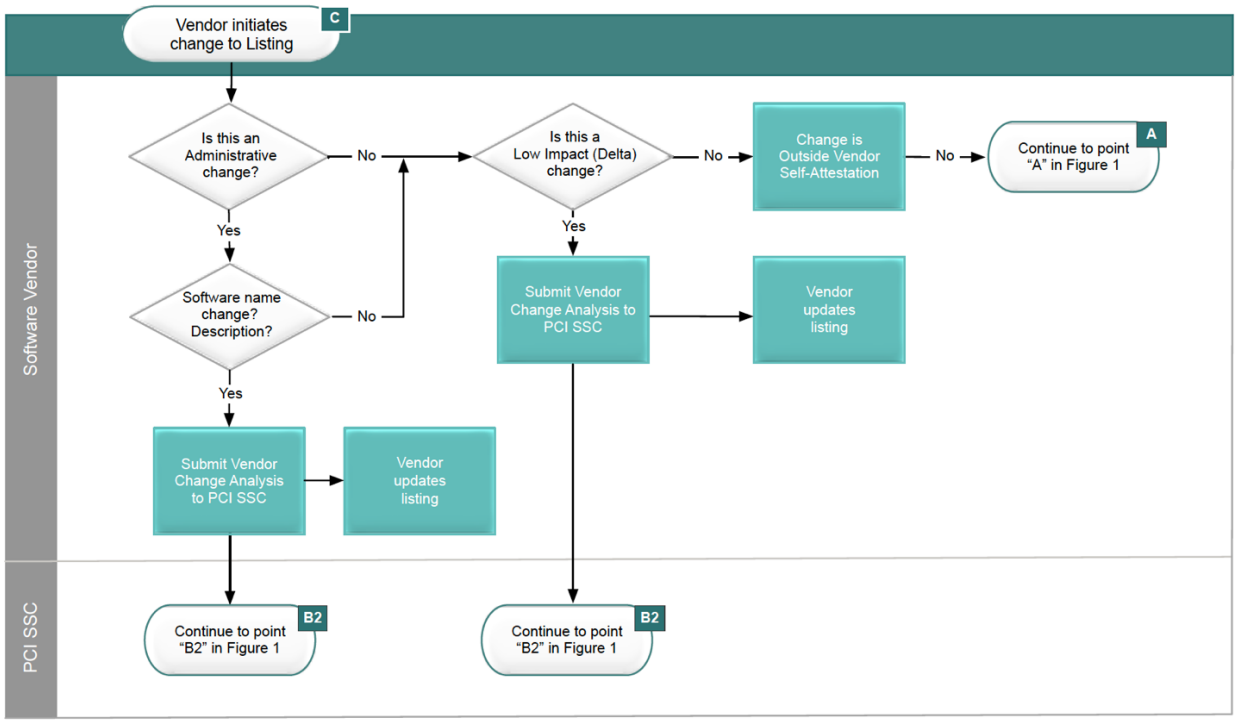


Figure 3b: Updates to Listed Payment Software – Secure SLC Qualified Vendor



5 Preparation for the Review

5.1 To what type of software does the PCI Secure Software Standard apply?

The PCI Secure Software Standard is intended for software vendors and others that develop Payment Software that is sold, distributed, or licensed to third parties. This includes Payment Software intended to be installed on customer systems as well as Payment Software sold, distributed, or licensed to third parties, regardless of how the software is delivered.

The PCI Secure Software Standard is not intended for Payment Software developed in-house for the sole use of the company that developed the software, nor is it intended for Payment Software developed and sold to a single customer for the sole use of that customer.

Examples of Payment Software	
ELIGIBLE for Validation Under the Secure Software Program	**INELIGIBLE for Validation Under the Secure Software Program**
▪ Software products involved in or directly supporting or facilitating payment transactions that store, process, or transmit clear-text account data. ▪ Software products developed by the vendor that are commercially available for sale to multiple organizations.	▪ In-house developed Payment Software that is used only by the company that developed it. ▪ Payment Software that operates on any consumer electronic mobile device that is not solely dedicated to payment acceptance for transaction processing. ▪ Payment Software intended for use on hardware terminals (e.g., PTS POI devices). ▪ Commercial operating systems onto which Payment Software may be installed, unless the operating system is an integrated component of the Payment Software itself. ▪ Commercial database applications that Payment Software may utilize for storage of account data, unless the database is an integrated component of the Payment Software itself. ▪ Other types of commercial software developed for purposes unrelated to transaction processing or Payment Software security characteristics, controls, features, and functionalities—for example, system monitoring or network management services—that may be in the same environment as the Payment Software but are not integrated components of the Payment Software.

Note: *PCI SSC will only Accept (defined in the VRA) and list Payment Software that is eligible for Secure Software Assessment, as determined by PCI SSC. Eligibility requirements will change as new modules are added to the PCI Secure Software Standard.*

5.2 Prior to the Review

Prior to commencing a Secure Software Assessment with a Secure Software Assessor Company, Vendors are encouraged to take the following preparatory actions:

- Determine/assess the PCI Secure Software Standard for modules applicable to the Payment Software;
- Determine/assess the Payment Software's readiness to comply with the PCI Secure Software Standard:
  - Perform a gap analysis between the Payment Software's security functionality and the Secure Software Requirements;
  - Correct any gaps; and
  - If desired, the Secure Software Assessor Company may perform a pre-assessment or gap analysis of a Vendor's Payment Software. If the Secure Software Assessor Company notes deficiencies that would prevent a compliant result, it may provide to the Vendor a list of Payment Software features to be addressed before the formal review process begins; and
- Determine whether the Vendor's *Security Guidance* meets the corresponding requirements of the PCI Secure Software Standard and make any necessary revisions.

5.3 Required Documentation and Materials

In connection with each Assessment, the Vendor must provide the appropriate documentation and software to the Secure Software Assessor Company.

All published PCI SSC information and documents relevant to the PCI Software Security Framework are available on the Website.

All completed Payment Software-related materials, such as install media (if applicable), manuals, the Vendor's *Security Guidance*, the Vendor Release Agreement, and all other materials related to the Assessment must be delivered to the Secure Software Assessor Company performing the Assessment, not to PCI SSC.

Examples of software, documentation, and other items to submit to the Secure Software Assessor Company include, but are not limited to:

1. The Payment Software;
2. The necessary hardware and software accessories to perform:
   - Simulated payment transactions; and
   - Operational support functions on the Payment Software
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 authorization, settlement and chargeback flows (if applicable to the software) must be described. A manual is an example of documentation that could fulfill this requirement.

4. Documentation that relates to installing, configuring, and operation of the Payment Software, or that provides information about the Payment Software. Such documentation includes but is not limited to:
   - Software Implementation guidance
   - Software Installation Guide or instructions (as provided to customers);
   - Vendor's software versioning methodology for the Payment Software;
   - Vendor's Vulnerability Handling Policies; and
   - Change control documentation that shows how changes are illustrated to customers
5. Additional documentation—such as diagrams and flowcharts—that will aid in the Assessment review; and
6. The Vendor's executed VRA (if PCI SSC does not already have a copy of the then-current version of the VRA signed by the Vendor).

Note: *The Secure Software Assessor Company may request additional Vendor materials as necessary.*

5.4 Secure Software Assessment Timeframes

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

- How close the Payment Software is to being PCI Secure Software Standard compliant at the start of the Assessment.
- Delays resulting from necessary Payment Software corrections to achieve compliance.
- Whether the Vendor's Security Guidance meets all Secure Software Requirements at the start of the Assessment.
  - Extensive rewrites of the Security Guidance will delay validation.
- Prompt payment of the fees due to PCI SSC.
  - PCI SSC will not commence the review of the ROV until the applicable fee has been paid.
- Quality of the Secure Software Assessor Company's submission to PCI SSC
- Delays resulting from incomplete submissions or those containing errors—for example, missing or unsigned documents, incomplete or inconsistent submissions.
- If PCI SSC reviews the ROV more than once, providing comments back to the Secure Software Assessor Company to address each time, this will increase the length of time for the review process.

Any Assessment timeframes provided by a Secure Software Assessor Company should be considered estimates. Problems found during the review or acceptance process, discussions required between the Secure Software Assessor-Employee, the Vendor, and/or PCI SSC, or other matters may significantly impact review times and cause delays and/or may even cause the review to end prematurely (for example, if the Vendor decides it does not want to make the necessary changes to achieve compliance or it is determined that the software is not eligible for PCI Secure Software Standard validation).

5.5 Secure Software Assessor Employees

PCI SSC qualifies Secure Software Assessor Companies and their Secure Software Assessor Employees to assess and validate Payment Software for compliance with the PCI Secure Software Standard. Additionally, PCI SSC provides required training for Secure Software Assessor Employees. In order to perform Secure Software Assessments, a Secure Software Assessor Company must:

- Have been qualified by PCI SSC;
- Have at least one Secure Software Assessor Employee;
- Ensure that both the Secure Software Assessor Company and Secure Software Assessor Employee remain in good standing; and
- Ensure that all Secure Software Assessor Employees complete all required Secure Software Assessor Employee training.

***Note**: A Secure Software Assessor Company may participate in one or more of the PCI Programs associated with the PCI Software Security Framework. The PCI Programs in which a Secure Software Assessor Company is a Qualified participant are included within the Assessor Company listing on the Website.*

All recognized Secure Software Assessor Companies are listed on the Website. Only Secure Software Assessor Employees of a Secure Software Assessor Company that meets the above criteria are recognized by PCI SSC as qualified to perform Secure Software Assessments.

- For each Secure Software Assessment, the resulting Assessment report must follow the ROV Report Template and corresponding instructions outlined in the ROV Report Template.
- The Secure Software Assessor Company must prepare each ROV based on evidence obtained by following the PCI *Secure Software Standard.*
- Each ROV must be accompanied by a Secure Software Attestation of Validation (AOV):
  - In the form available through the Website;
  - Signed by a duly authorized officer of the Secure Software Assessor Company;
  - Summarizing whether the evaluated Payment Software is in compliance or is not in compliance with the PCI Secure Software Standard, along with any related findings.

5.5.1 Use of the Secure Software Assessor Company Environment

Secure Software Assessor Companies are required to test Payment Software in a pristine computing environment, free from potentially conflicting applications, network traffic, security and/or access controls, software versions, and artifacts or "orphaned" components left behind from other software installations. The testing environment must be set up—and capable of being repeatedly reset—as a predictable, clean environment. If reusing a testing environment previously configured for testing a different Payment Software product or different version of the same Payment Software product, due diligence must be carried out to ensure that any ghost/orphaned permissions, accounts, registry settings, DLLs, security settings, etc., left over from the previous installation have been removed. Any dependencies (for example, operating systems, databases, firewalls, routers, anti-malware software, intrusion detection/prevention, and file integrity monitoring, etc.) must restore permissions, accounts, access, stored procedures, etc., to a known, predictable, and/or original state.

***Note:** Remote access—using multi-factor authentication—to the testing environment is acceptable.*

For each Secure Software Assessment, Secure Software Assessor Company testing environment processes must include:

- Using the Vendor's installation manual, training provided, and the *Security Guidance* to perform the default installation of the Payment Software.
- Confirming that all implementations of the Payment Software (including region/country specific versions) to be listed were tested in the testing environment.
- Confirming that all Payment Software versions and platforms to be listed were tested, including all necessary system components and dependencies.
- Confirming that all critical Payment Software functionalities were tested.
- Confirming that the testing environment is capable of simulating the "real world" use of the Payment Software, including:
  - Ensuring that production data (live PAN) is not used for testing and development
  - Confirming that the testing environment is capable of running authorization and/or settlement functions and that processes include examination of output from all functions.
- Confirming that the testing environment is capable of simulating and validating all functions of the Payment Software, including the testing environment's capability to exploit software vulnerabilities.
- Use of the Secure Software Assessor Company's Testing Environment requires the submission of the Testing Environment Configuration for Secure Software Assessments, found in ROV Reporting Template Appendix B, with each Secure Software Assessment. This form includes a description for the environment configuration as part of each Secure Software Assessment.
- In the event that the Secure Software Assessor Company Testing Environment is not capable of properly and fully testing all functions of the Payment Software, an alternative environment may be used. Testing Payment Software in an alternative environment also requires completion of ROV Reporting Template, Appendix B: Testing Environment Configuration for Secure Software Assessments, for each Secure Software Assessment where an alternative environment is used.

5.5.2 Secure Software Assessor Company Fees

The prices and fees charged by Secure Software Assessor Companies are not set by PCI SSC. These fees are negotiated between the Secure Software Assessor Company and its customers (i.e., Vendors seeking to have their Payment Software validated against the PCI Secure Software Standard). Before deciding on a Secure Software Assessor Company, it is recommended that the Vendor check PCI SSC's list of Secure Software Assessor Companies on the Website, talk to several Secure Software Assessor Companies, and follow its own vendor-selection processes.

5.5.3 Other Software Assessment Services Offered by Secure Software Assessor Companies

The list below provides examples of other Software Assessment services that may be offered by Secure Software Assessor Companies. These services are neither required nor recommended by PCI SSC. If these services are of interest to your company, please contact the Secure Software Assessor Companies for availability and pricing. Examples of other Software Assessment services include:

- Providing guidance on designing Payment Software in accordance with the PCI Secure Software Standard.
- Reviewing a Vendor's software design, response to questions via e-mail or phone, and participation in conference calls to clarify requirements.
- Providing guidance on preparing the *Security Guidance*.
- Providing pre-assessment (gap analysis) services prior to beginning formal Secure Software Assessment.
- Providing guidance for bringing the Payment Software into compliance with the PCI Secure Software Standard if gaps or areas of non-compliance are noted during the assessment.

Note: *When arranging for other Software Assessment services with a Secure Software Assessor Company, care should be taken by both the Vendor and the Secure Software Assessor Company to ensure that the Secure Software Assessor Company maintains all independence requirements as set forth in the SSF Qualification Requirements—for example, that a Secure Software Assessor Company does not, as part of the Secure Software Assessment, assess its own work product previously provided to the applicable customer. Conflicts of interest may result in a Vendor's Secure Software Assessment being rejected by PCI SSC.*

5.6 Technical Support throughout Testing

To expedite the Evaluation process, it is recommended that the Vendor designate an individual with sufficient technical knowledge to act as a liaison throughout the review, providing assistance with any questions that may arise. The Vendor's designated contact should be on call to discuss issues and respond to questions from the Secure Software Assessor Company.

5.7 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 Secure Software Assessor Company along with the secure software process and other documents and materials at the beginning of each Secure Software Assessment, and must be provided to PCI SSC by the Secure Software Assessor 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 Secure Software Program requirements, policies, and procedures, and gives permission to the Vendor's Secure Software Assessor 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.

Note: *A ROV will not be reviewed by PCI SSC without the then-current VRA on file from the relevant Vendor. However, so long as the executed current VRA is on file with PCI SSC for the relevant Vendor, it is not required to re-submit the same VRA with each subsequent ROV for the same Vendor.*

5.8 Secure Software Acceptance Fees

Vendors are also required to pay a *Secure Software Acceptance Fee* to PCI SSC. For each new Payment Software submission, the Secure Software Acceptance Fee will be invoiced and must be received by PCI SSC before the submission will be reviewed and (if appropriate) Accepted (defined in the VRA) and added to the List of Validated Payment Software. Upon Acceptance, the PCI SSC will sign and return a copy of the completed Secure Software Attestation of Validation (AOV) to both the Vendor and the Secure Software Assessor Company.

There are no annual recurring PCI SSC fees associated with the Acceptance of a Validated Payment Software product. There are, however, PCI SSC fees associated with updates to Validated Payment Software products. Please see the Website for more information.

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

***Note**: The Vendor pays all Secure Software Assessment-related fees directly to the Secure Software Assessor Company (these fees are negotiated between the Vendor and the Secure Software Assessor Company).*

PCI SSC will bill the Vendor for all Payment Software Acceptance Fees and the Vendor will pay these fees directly to PCI SSC.

6 Managing Validated Payment Software

Subject to early expiry and the terms of the VRA, the version of the Payment Software that was successfully validated by the Secure Software Assessor Company and Accepted by PCI SSC will be listed as Validated Payment Software for a period of three years from the date of Acceptance of that version.

Note: *PCI SSC reserves the right to withdraw Acceptance as indicated in Section 2.5.*

6.1 Annual Attestation

Annually, by the revalidation date noted on the List of Validated Payment Software, the Vendor is **required** to submit an updated *Secure Software Attestation of Validation (AOV)* to PCI SSC. The Vendor must perform the Annual Requalification steps as indicated in Part 2 of the AOV.

Note: *Annual Attestations will be accepted no more than 90 days prior to revalidation date.*

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

- Confirm that Validated Payment Software continues to meet all applicable *Secure Software* requirements; and
- Confirm that changes made apply in a way that is consistent with the documented software versioning methodology for that Validated Payment Software product; and
- Notify PCI SSC of any changes made to the Payment Software that necessitate a change to its listing on the Website.

The Vendor is required to consider the impact of external threats, including changes to the environment in which the Payment Software operates. This includes the tested platforms, operating systems, and any required dependencies the software may have. For Validated Payment Software, Vendors are required to confirm that all tested platforms, operating systems, and dependencies upon which the Validated Payment Software relies remain supported—for example, that the Vendor (of the operating system, databases, dependent software, etc.) continues to maintain and provide updates for any security vulnerabilities identified. If any tested platform, operating system, or dependency is no longer supported at the time of the Annual Revalidation, this must be reflected in the Vendor's response to PCI SSC and will result in an updated listing on the Website to indicate the validation has expired.

Note*: If an updated AOV is not submitted for a Validated Payment Software product, that Payment Software will be deemed to have suffered an early administrative expiry. As such, the List of Validated Payment Software will be amended to identify that the validation of Payment Software has expired.*

PCI SSC will, upon receipt of the updated *AOV*: (i) review the submission for completeness; (ii) once completeness is established, update the List of Validated Payment Software with the new requalification date; and (iii) sign and return a copy of the updated *AOV* to the applicable Vendor.

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

6.2 Changes to Listed Payment Software

Vendors may wish to update listed Payment Software for various reasons—for example, adding/removing auxiliary functionality, maintaining security updates, or upgrading the baseline or core Payment Software. The table below provides a summary of the three types of change scenarios from a Secure Software Program perspective:

Change Type	Description
Administrative	Changes to the Validated Payment Software listing or changes to how the Payment Software is described in the List of Validated Payment Software, for example, corporate identity or application name changes. *See Section 6.2.1.1, "Administrative Changes," for details.*
Low Impact	Low Impact changes to the Payment Software include any changes to the software architecture, source code, or components that do not trigger High-impact Change criteria. Low Impact changes may be eligible for partial or "delta" assessment. *See Section 6.2.1.2, "Low Impact Changes," for details.*
High Impact	High Impact changes to the Payment Software include any changes to the software architecture, source code, or components that handle or interact with Sensitive Data, Sensitive Functions, or Sensitive Resources. High Impact changes require the Vendor to submit the new version of the Payment Software for a full Secure Software assessment. *See Section 6.2.1.3, "High Impact Changes," for details.*

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

6.2.1 Change Types

The following sections provide details about changes to Validated Payment Software, the supporting documentation that must be generated, and the processes to be followed in order to successfully effect changes to the listing of Validated Payment Software.

The process flow for changes to listings for Validated Payment Software is detailed in Figure 4.

6.2.1.1 Administrative Changes

Administrative changes are limited to updates where no actual software changes have occurred, but the Vendor wishes to make a change to the corresponding listing on the List of Validated Payment Software. Administrative changes include, but are not limited to, changes to the Payment Software name or Vendor's corporate entity name.

If the Vendor *is* a Secure SLC Qualified Vendor, the following steps are used to update the List of Validated Payment Software:

- Completion of a Self-Assessment to confirm the change type and submission of a Self-Attestation to PCI SSC for review;
- The Vendor amends the List of Validated Payment Software accordingly with the new information; and
- PCI SSC will then sign and return a copy of the Self-Attestation to the Vendor.

If the Vendor is *not* a Secure SLC Qualified Vendor, the following steps are used to update the List of Validated Payment Software.

***Note**: Secure SLC Qualified Vendors are only allowed to update the List of Validated Payment Software for software developed using their PCI SSC-qualified software lifecycle management practices.*

Any Payment Software developed using other practices may only be updated according to steps outlined for Vendors who are not Secure SLC Qualified Vendors.

- Completion of a Self-Assessment to confirm the change type and submission of a Self-Attestation to PCI SSC for review.
- PCI SSC will then:
  - Issue an invoice to the Vendor for the applicable change fee;
  - Upon payment of the invoice, review the Self-Attestation for quality assurance purposes;
  - Amend the List of Validated Payment Software on the Website accordingly with the new information; and
  - Sign and return a copy of the Self-Attestation to the Vendor.

***Note**: The update process does not alter the Expiry Date (See Section A.9 of Appendix A below) of updated Payment Software, which is set at three years after the date on which the applicable version of the product was first Accepted.*

PCI SSC reserves the right to reject any Change Impact document if it determines that a change described therein and purported to be an Administrative Change by the Vendor is ineligible for treatment as an Administrative Change.

6.2.1.2 Low Impact Changes

Low Impact changes to Validated Payment Software products are eligible for partial re-assessment or “delta” assessment. Low Impact changes do not handle sensitive data, functions, and resources that would trigger a High Impact Change.

Vendors are afforded some flexibility for Delta Assessments, depending upon the type of update made to the Payment Software. If the Vendor of the Validated Payment Software is *not* a Secure SLC Qualified Vendor, all updates to the Validated Payment Software must be reviewed by a Secure Software Assessor to confirm the scope of the change. Vendors who have been validated to the PCI Secure SLC Standard through a Secure SLC Assessment are afforded greater flexibility during the Delta Assessment process.

Whether performed by a Secure Software Assessor or by the Secure SLC Qualified Vendor, all Delta Assessments must:

- Include all requirements of the PCI Secure Software Standard ("Requirements") affected by the change in the Change Impact Analysis;
- Include verification that all other Requirements are not affected by the change;
- Include details about how, for all Requirements not included in the Delta Assessment:
  - The Secure Software Assessor verified that those Requirements were *not* affected by the change, OR
  - The Secure SLC Qualified Vendor verified that those Requirements were *not* affected by the change;
- Include Payment Software functionality testing; and
- Be completed using the same version of the PCI Secure Software Standard, any and all applicable appendices, as were used for the full validation—for example, a Validated Payment Software product originally validated against PCI Secure Software Standard v1.0 cannot have a delta assessment performed using PCI Secure Software Standard v2.0, and vice-versa.

***Note**: In all Delta Change cases that require assessment or review by a Secure Software Assessor, the Vendor must ensure that these activities are performed by the same company that performed the last Full Assessment and validation of the Payment Software.*

Figure 4 provides a high-level overview of the software validation process for Secure SLC Qualified Vendors and those Vendors who are not Secure SLC Qualified.

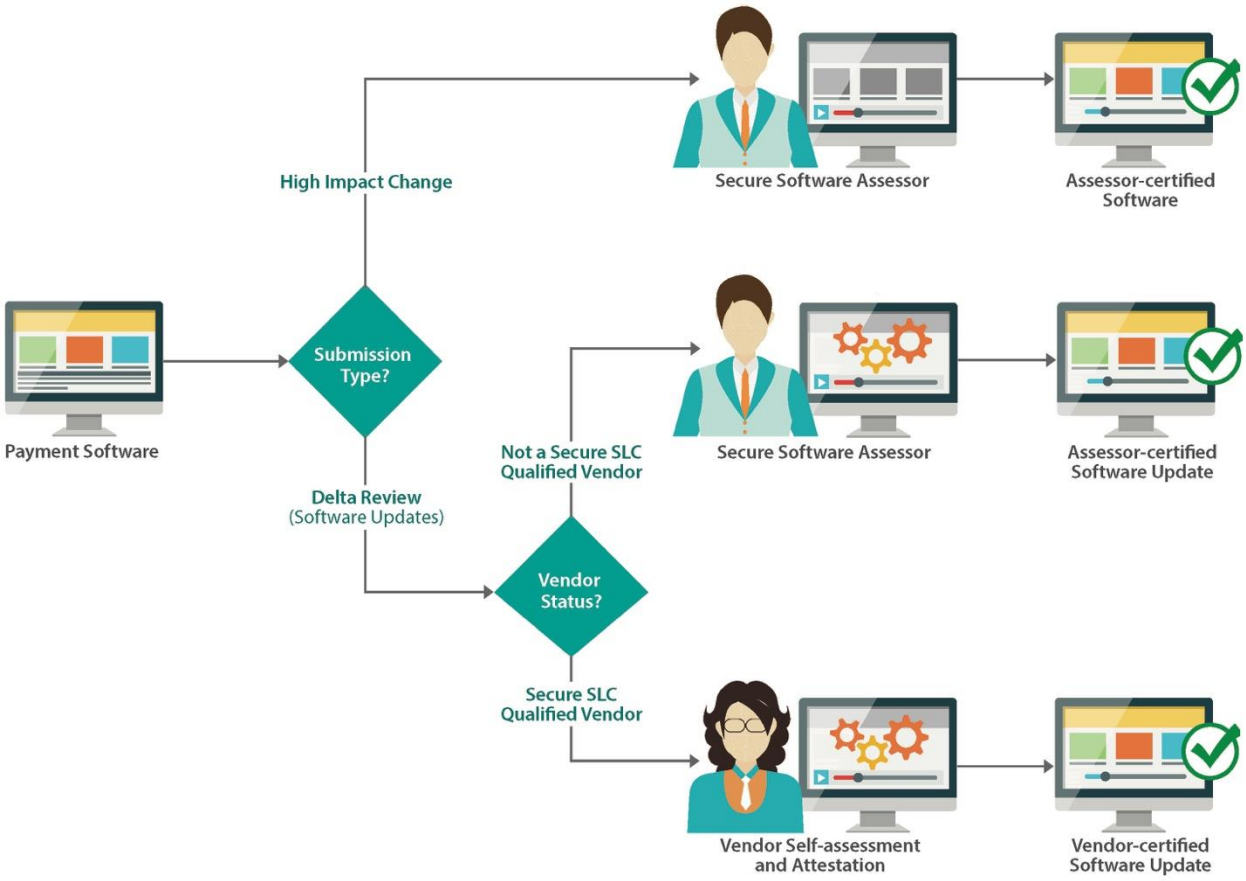


Figure 4: Software Validation Workflow

If the Vendor *is* a Secure SLC Qualified Vendor, the Vendor must perform the following actions to update the List of Validated Payment Software (see Table 1):

- Perform a Self-Assessment to confirm the change type, then submits a Self-Attestation to PCI SSC for review;
- Amend the List of Validated Payment Software accordingly with the new information; and

PCI SSC will then sign and return a copy of the Self-Attestation to the Vendor.

If the Vendor is *not* a Secure SLC Qualified Vendor, the Vendor must perform the following actions to update the List of Validated Payment Software (see Table 2):

- Performs a Self-Assessment to confirm the change type, then submits a Self-Attestation to Secure Software Assessor Company for review.

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

- Notifies the Vendor that it agrees;
- Performs a delta review of the Payment Software for the Secure Software Requirements affected by the Low Impact change;

- Tests the Payment Software's functionality;
- Completes a Vendor Change Impact document in Appendix C and makes redline changes to the original ROV as appropriate;
- Signs its concurrence on the Attestation of Validation and forwards it—along with the "redline" version of the ROV, the Payment Software's updated installation guidance, and the Vendor Change Impact document to PCI SSC.

PCI SSC will then:

- Issue an invoice to the Vendor for the applicable change fee;
- Upon payment of the invoice, review the Self-Attestation, the "redline" version of the ROV and the Vendor Change Impact document for quality assurance purposes;
- Amend the List of Validated Payment Software accordingly with the new information; and
- Sign and return a copy of the Self-Attestation to the Vendor and the Secure Software Assessor.

For quality issues associated with any aspect of the submission, PCI SSC communicates those issues to the Secure Software Assessor Company, and those issues are resolved according to the process depicted in Figure 1.

***Note**: The update process does not alter the Expiry Date of updated Payment Software, which is set at three years after the date on which the applicable version of the product was first Accepted.*

PCI SSC reserves the right to reject any Change Impact document if it determines that a change described therein and purported to be a Low Impact Change by the Vendor is ineligible for treatment as a Low Impact Change.

6.2.1.3 High Impact Changes

High Impact changes to the Payment Software include:

- Any changes to the software architecture, source code, or components that handle or interact with Sensitive Data, Sensitive Functions, or Sensitive Resources.
- The addition of a tested platform/operating system to include on the List of Validated Payment Software.

The Vendor performs an initial Self-Assessment to confirm the change type is a High Impact Change. If High Impact, the Vendor must seek a full software validation as described in Section 4.2, "Initial Validation and Listing."

***Note**: In all cases, Validation of a High Impact Change requires that the Vendor work with a PCI Secure Software Assessor Company. See Section 5 for further details.*

Table 1: Software Validation for Vendors who are not Secure SLC Qualified Vendors

Type of Software Submission	Software Validation Methods			Frequency of submission
	Assessment by PCI-qualified Secure Software Assessor Company	*Vendor Self-Assessment and Self-Attestation*	*Vendor Self-Assessment with Delta Review and Testing by PCI-qualified Secure Software Assessor Company*	
Initial/Full software validation	✓			Every three years (after initial validation)
High Impact change	✓			Upon implementation of change
Annual attestation for Validated Payment Software		✓		Annually
Administrative change		✓		Upon implementation of change
Low Impact change (Delta)			✓	

Table 2: Software Validation for Secure SLC Qualified Vendors

Type of Software Submission	Software Validation Methods		Frequency of submission
	Assessment by PCI-qualified Secure Software Assessor Company	*Vendor Self-Assessment and Self-Attestation*	
Initial/Full software validation	✓		Three years from date of PCI SSC Acceptance.
High Impact change	✓		Upon implementation of change
Annual attestation for Validated Payment Software		✓	Annually
Administrative change		✓	Upon implementation of change
Low Impact change (Delta)		✓	

6.2.2 Change Documentation

Administrative Change	Low Impact Change	High Impact Change or New Payment Software
Software Vendor		
▪ *Attestation of Validation* ▪ *Vendor Release Agreement* (one per Vendor) * ▪ Fee	▪ *Attestation of Validation* ▪ Report on Validation (Redline version) ▪ *Security Guidance* ▪ Fee	▪ *Attestation of Validation* ▪ Report on Validation ▪ *Security Guidance* ▪ *Vendor Release Agreement* (one per Vendor) * ▪ *Change Impact Analysis** ▪ Fee
Secure SLC Qualified Vendor		
▪ *Attestation of Validation* ▪ Report on Validation ▪ *Security Guidance* ▪ *Vendor Release Agreement* (one per Vendor) * ▪ Fee*	▪ *Attestation of Validation* ▪ Report on Validation ▪ *Secure Software Implementation Guidance* ▪ *Vendor Release Agreement* (one per Vendor) * ▪ Fee*	▪ *Attestation of Validation* ▪ Report on Validation ▪ *Security Guidance* ▪ *Vendor Release Agreement* (one per Vendor) * ▪ *Change Impact Analysis** ▪ Fee

** If applicable*

***Note**: The Secure Software Change Impact document in Appendix C is mandatory for the Secure Software Assessor Company for submitting Administrative, No Impact, Low Impact and High Impact changes to PCI SSC but may also be used by Secure SLC Qualified Vendors as a Vendor Change Analysis.*

6.2.3 Renewing Expiring Payment Software

As a Payment Software product approaches its Expiry Date, PCI SSC will notify the Vendor of the pending expiration. The two options available for Vendor consideration in connection with expiring Payment Software are either new validation or expiry:

- **New Validation**: If the Vendor wishes the Payment Software to remain on the List of Validated Payment Software, the Vendor must contact a Secure Software Assessor Company to have the Payment Software fully re-evaluated against the then-current version of the PCI Secure Software Standard and any modules which are then applicable for the Payment Software. Use of the Low or Administrative Change process to achieve this goal is not permitted.

***Note**: Vendors are allowed to voluntarily elect to move Payment Software to an "expired" status by submitting an Attestation and request.*

Secure SLC Qualified Vendors may make this change themselves on the Portal and submitting the Attestation to PCI SSC.

- **Expiry**: Upon expiration of the Payment Software's listing on the Website, the Payment Software must be resubmitted for a Full Software Assessment in order to retain its validation. Payment Software that is not resubmitted for revalidation will be identified on the PCI SSC website as "expired".

Note that if the expiring Payment Software successfully completes the Secure Software Assessment process again, the re-validated Payment Software retains its status on the List of Validated Payment Software and is assigned a new Expiry Date.

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

6.2.4 Validation Maintenance Fees

If a Validated Payment Software listing is revised, the Vendor is required to pay the applicable change fee to PCI SSC.

For any change affecting the listing of Validated Payment Software, the applicable fee will be invoiced and must be received by PCI SSC for the changes to be Accepted and added to the List of Validated Payment Software. Upon Acceptance, PCI SSC will sign and return a copy of the AOV to both the Vendor and the Secure Software Assessor Company.

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

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

***Note**: The Vendor pays all Secure Software Assessment-related fees directly to the Secure Software Assessor Company (these fees are negotiated between the Vendor and the Secure Software Assessor Company).*

PCI SSC will invoice the Vendor for all validation maintenance fees and the Vendor will pay these fees directly to PCI SSC.

Secure SLC Qualified Vendors are not required to pay validation maintenance fees for Administrative and Low Impact changes.

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

In the event of a Security Issue (defined in the VRA) relating to Validated Payment Software, the VRA requires the applicable Vendor to notify PCI SSC. *Vendors must be aware of and adhere to their obligations under the VRA in the event of a Security Issue.*

7 Secure Software Assessment Reporting Considerations

7.1 Secure Software Assessment Acceptance Process Overview

The Secure Software Assessor Company performs the Secure Software Assessment in accordance with the Secure Software Requirements, and produces a ROV that is shared with the Vendor. If the ROV does not have all items in place, the Vendor must address those items, and the Secure Software Assessor Company must update the ROV prior to submission to PCI SSC. For example, this may include updating user documentation or software. Once the Secure Software Assessor Company is satisfied that all documented issues have been resolved by the Vendor, the Secure Software Assessor Company submits the ROV and all other required materials to PCI SSC through the secure submission website designated by PCI SSC for the Program (the "Portal"), described further in Section 7.2 below.

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

Once PCI SSC receives the ROV and all other required materials and applicable fees, PCI SSC reviews the ROV from a quality assurance perspective, typically within 30 calendar days of payment of invoice, and determines whether it is acceptable. Subsequent iterations will also be responded to, typically within 30 calendar days of receipt. If the ROV meets all applicable quality assurance requirements (as documented in the SSF Qualification Requirements and related Program materials), PCI SSC sends a countersigned AOV to both the Vendor and the Secure Software Assessor Company, and adds the Validated Payment Software to the List of Validated Payment Software.

***Note**: It is common for submissions to require several iterations before the Payment Software is Accepted. Adequate QA review of the submission as part of the Secure Software Assessor Company's internal QA process will help minimize the number of iterations required. Each iteration will be responded to typically within 30 days from the time that iteration was received in the Portal.*

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

ROVs that have been returned to the Secure Software Assessor Company for correction must be resubmitted to the PCI SSC within 30 days of the preceding submittal. If this is not possible, the Secure Software Assessor Company must inform the PCI SSC of the timeline for response and PCI SSC may grant an extension. Lack of response on ROVs returned to the Secure Software Assessor Company for correction may result in the submission being closed. Submissions that have been closed will not be reopened and must be resubmitted as if they are new ROV submissions.

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

7.2 Delivery of the ROV and Related Materials

All documents required in connection with the Secure Software Program validation process must be submitted to PCI SSC by the Secure Software Assessor Company, through the Portal. PCI SSC will pre-screen Portal submissions to ensure that all required documentation has been included and the submission requirements have been satisfied.

There must be consistency between the information in documents submitted for review via the Portal and the "Details" fields within the Portal. Common errors in submissions include inconsistent Payment Software names or contact information, incomplete or inconsistent documentation, Payment Software dependencies being insufficiently explained, and tested platforms/operating systems being insufficiently explained. Incomplete or inconsistent submissions may result in significant delays in processing submissions and/or may not be Accepted for review by the PCI SSC.

Access to the Portal

Access to the Portal is granted to qualified Secure Software Assessor Companies. Secure Software Assessor Employees receive log-on instructions upon passing the Secure Software Assessor-Employee training exam. The Primary Contact for a Secure Software Assessor Company must be a Secure Software Assessor-Employee and receive higher-level access to the Portal than Secure Software Assessor Employees who are not the Primary Contact, in order to enable the Primary Contact to manage Secure Software Assessor Company-related tasks. Access is granted to the Primary Contact upon e-mail request to the PCI SSC Software Security Framework Program Manager.

Listing Information

The List of Validated Payment Software will contain, at minimum, the information specified below. Each characteristic is detailed in Appendix A, "Payment Software Elements," for the AOV and the List of Validated Payment Software.

- Payment Software Vendor
- Payment Software Identifier
  - Payment Software Name
  - Payment Software Version Number
  - Payment Software Type
- Reference Number
- Description provided by Vendor
- Tested platforms/operating systems
- Required dependencies
- Validation notes (PCI Secure Software Standard version)
- Deployment notes
- Revalidation Date
- Expiry Date
- Secure Software Assessor Company

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

7.3 Assessor Quality Management Program

Secure Software Assessor Companies are required to meet all QA standards set by PCI SSC. The various phases of the PCI SSC Assessor Quality Management (AQM) program for Secure Software Assessor Companies are described below.

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

ROV Submission Reviews

PCI SSC's AQM program 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.

If the Payment Software is determined to be eligible for validation under the Secure Software Program and the submission is complete, the AQM analyst will complete a full review of the ROV submission and all supporting documentation provided or requested as part of the initial submission or subsequently thereafter. Any comments or feedback from the AQM analyst will be made via the Portal, and the Secure Software Assessor 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 Secure Software Assessor Company's submission to provide reasonable assurance that a quality Assessment was performed.

Secure Software Program Quality Audit

The purpose of the Secure Software Assessor Company audit process is to provide reasonable assurance that the Assessment of Payment Software and overall quality of report submissions remain at a level that is consistent with the requirements and objectives of the Program, the Program Guide, and supporting PCI SSC documentation.

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

Secure Software Assessor Company Status

The Secure Software Program recognizes several status designations for Secure Software Assessor Companies: "In Good Standing," "Remediation," and "Revocation." The status of a Secure Software Assessor 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: *Status designations are not necessarily progressive: Any Secure Software Assessor Company's status may be revoked or its SSF Agreement terminated in accordance with the terms of the SSF Agreement; and accordingly, if warranted, a Secure Software Assessor Company may move directly from "In Good Standing" to "Revocation."*

All status designations are defined in the SSF Qualification Requirements and the SSF Agreement.

However, in the absence of severe quality concerns, Secure Software Assessor Companies with quality issues are generally first addressed through the Remediation process in order to promote improved performance.

7.3.1.1 In Good Standing

Secure Software Assessor Companies are expected to maintain a status of In Good Standing while participating in the Secure Software 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 Secure Software Assessor Company may also be subject to periodic audit by PCI SSC at any time.

7.3.1.2 Remediation

A Secure Software Assessor Company may be placed into Remediation for various reasons, including quality concerns or administrative issues (such as failure to meet applicable requalification requirements, failure to submit required information or documentation). Secure Software Assessor Companies in Remediation are listed on the Website in red, indicating their Remediation status without further explanation as to why the designation is warranted.

If administrative or non-severe quality problems are detected, PCI SSC will generally recommend participation in the Remediation program. Remediation provides an opportunity for Secure Software Assessor Companies (and/or their Secure Software Assessor Employees) to improve performance by working closely with PCI SSC staff. Additionally, Remediation helps to assure that the baseline standard of quality for Secure Software Assessor Companies and/or Secure Software Assessor Employees is maintained.

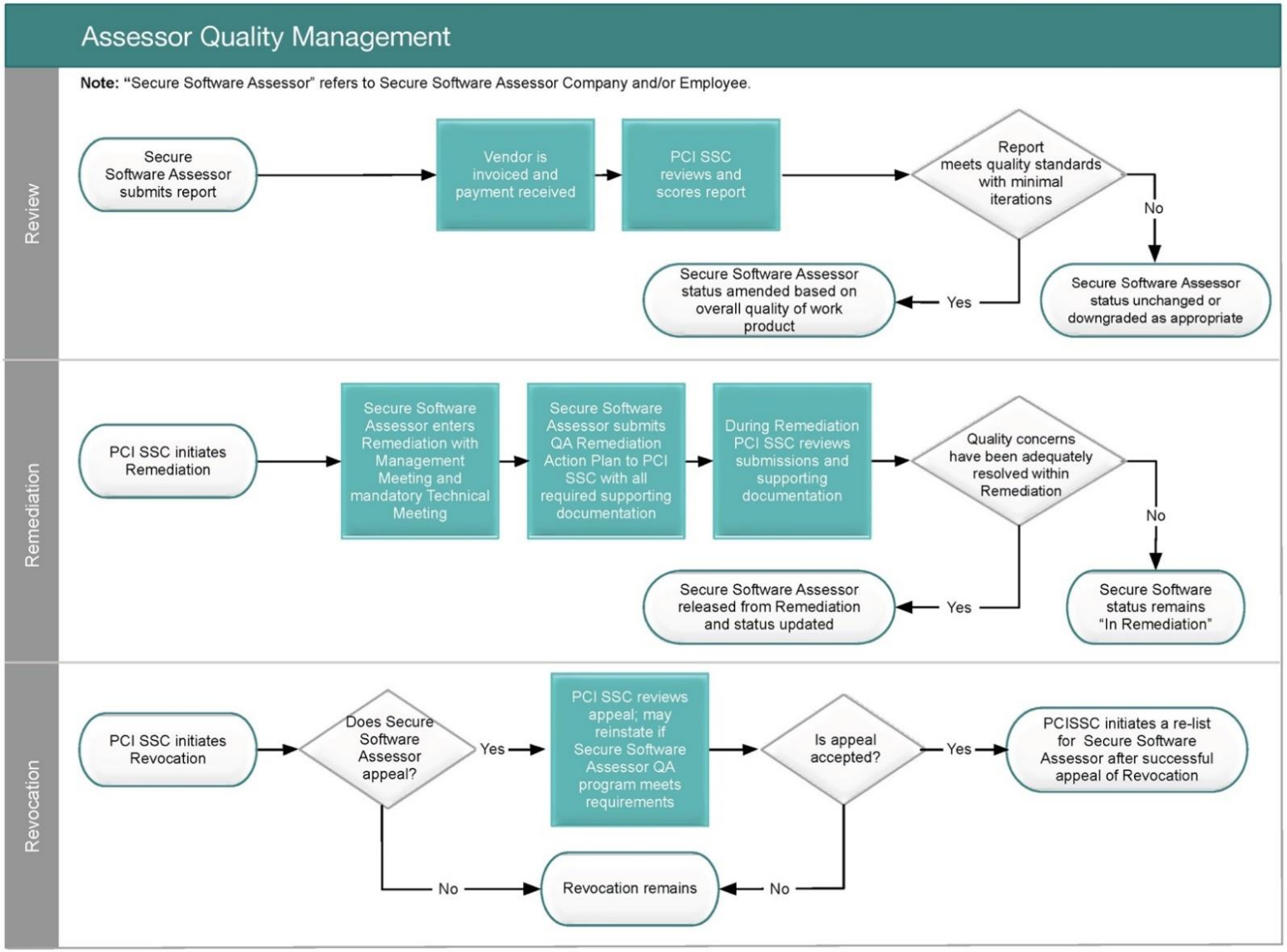
***Note**: If Validated Payment Software is compromised due to Secure Software Assessor Company and/or Secure Software Assessor Employee error, that Secure Software Assessor Company and/or Secure Software Assessor Employee may immediately be placed into Remediation or its status revoked.*

7.3.1.3 Revocation

Serious quality concerns, issues or problems may result in revocation of Secure Software Assessor Company and/or Secure Software Assessor Employee qualification and termination of the SSF Agreement. When a Secure Software Assessor Company's qualification is revoked, it and its Secure Software Assessor Employees are removed from the corresponding Program lists on the Website.

The Secure Software Assessor Company may appeal Revocation. However, unless otherwise approved by PCI SSC in writing in each instance, the Secure Software Assessor Company (and its Secure Software Assessor Employees) is not permitted to perform Secure Software Assessments, process ROVs, or otherwise participate in the Secure Software Program. The Secure Software Assessor Company may reapply one year after revocation, so long as it has demonstrated to PCI SSC's satisfaction that it meets all applicable Program requirements.

Figure 5: Secure Software Assessor Company QA Programs for Report Reviews



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

A.1 Payment Software Vendor

This entry denotes the Vendor of the Validated Payment Software.

A.2 Payment Software Identifier

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

- Payment Software Name
- Payment Software Version #
- Payment Software Type
- Reference Number

Example of a Payment Software Identifier:

Component	Description
Payment Software Name	Acme Payment 600
Payment Software Version #	PCI 4.53.x
Payment Software Type	POS Suite
Reference #	09-01.00111.001

Payment Software Identifier: Detail

- **Payment Software Name**

  Payment Software Name is provided by the Vendor and is the name by which the Validated Payment Software is sold. The Payment Software Name cannot contain any variable characters.

  Use of PCI SSC's name, standards, program names and/or associated acronyms (e.g., PCI DSS, SLC, Secure Software, PTS, etc.) in Payment Software Names is strictly prohibited. PCI SSC reserves the right to reject any Payment Software violating this naming policy.

- **Payment Software Version #**

  Payment Software Version # represents the Payment Software version reviewed in the Secure Software Assessment. The format of the version number:

  - Is set by the Vendor
  - May consist of alphanumeric characters

***Note**: See Appendix B: Payment Software Version Methodology for details about content to include in the Vendor's versioning methods.*

Customers are strongly advised to deploy only that Payment Software with the Payment Software Version # whose characters are consistent with the Payment Software Version # shown on the List of Validated Payment Software.

- **Payment Software Type**

  The Vendor must choose the option that best describes the primary function of the Payment Software from the list below:

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

Type	Function	Description
10	Card-Not-Present	Payment Software that is used by merchants to facilitate transmission and/or processing of payment authorization and/or settlement in card-not-present channels.
11	Automated Fuel Dispenser	Payment Software that provides operation and management of point-of-sale transactions, including processing and/or accounting functions in fuel dispensing environments.
12	Payment Module	Payment Software that operates as a component of a broader application environment upon which it is dependent to operate. Such software must have distinguishable configuration identifiers that are easily discernible from the broader application environment.

- **Reference Number**

  PCI SSC assigns the Reference number once the Payment Software is posted to the Website; this number is unique per Vendor and will remain the same for the life of the Payment Software'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 Software Type (see above)	2 digits + period
Vendor #	5 digits + period (assigned alphabetically initially, then as received)
Vendor App #	3 digits + period (assigned as received)
Minor change reference	3 alpha characters (assigned as received)

A.3 Tested Platforms/Operating Systems

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

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

A.4 Required Dependencies

Identify specific dependencies that the submitted Payment Software has to other Validated Payment Software, 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 Validated Payment Software or PTS reference numbers.

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

A.5 Validation Notes

Validation Notes are used by PCI SSC to denote what standard, and the specific version of the standard, was used to assess the compliance of a Validated Payment Software.

A.6 Deployment Notes

Deployment Notes are used by PCI SSC to identify the current status of Validated Payment Software for Program purposes. See table under "Expiry Date" below for examples.

Assigned deployment notes are determined based on the Payment Software's Expiry Date and/or the Vendor's timely completion of annual revalidation (whether or not the particular version of the Payment Software is still being supported by the Vendor).

Validated Payment Software is denoted with one of the following Deployment Notes:

- **Validated Payment Software**: All newly Accepted Validated Payment Software is initially denoted as "Validated Payment Software" and will retain this designation until denoted as "Expired Payment Software."
- **Expired Payment Software**: This deployment note is assigned to Validated Payment Software when either (i) annual revalidation requirements are not satisfied by the Vendor, causing early administrative expiry, or (ii) the Validated Payment Software reaches its Expiry Date (based on the version of the PCI Secure Software Standard under which it was validated).

  Please refer to specific payment card brand requirements for questions or information regarding usage of Validated Payment Software and Expired Payment Software.

A.7 Annual Attestation Date

Validated Payment Software must be revalidated annually. The **Annual Attestation Date** is used by PCI SSC to indicate when the Vendor's annual Attestation of Validation is due. The Revalidation Date is specified on the Attestation of Validation.

A.8 Expiry Date

The **Expiry Date** for Validated Payment Software is the date by which a Vendor must have the Payment Software re-evaluated against the then-current version of the PCI Secure Software Standard in order to maintain Acceptance.

Note: *Each payment card brand develops and enforces its own compliance program for usage of Validated Payment Software, including, but not limited to requirements, mandates, and/or dates for use of Validated Payment Software; fines or penalties related to use of non-compliant Payment Software; and other requirements for using Payment Software. Questions on how the use of products denoted as Expired Payment Software may affect PCI DSS compliance should be addressed to the merchant's acquirer and/or the affected payment card brands.*

Example Listing Format for Validated Software

Validation Notes	Expiry Date	Deployment Notes	Annual Attestation Date
Validated According to PCI Secure Software Standard v1.0	28 October 2023	Validated or Expired	28 October 2022

A.9 Secure Software Assessor Company

This entry denotes the name of the Secure Software Assessor Company that performed the validation and determined that the Payment Software is compliant with the PCI SSC Secure Software Standard.

Appendix B: Payment Software Versioning Methodology

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

B.1 Version Number Format

The format of the Payment Software version number is set by the Vendor and may be comprised of several elements. The versioning methodology must fully describe the format of the Payment Software version number including the following:

- The format of the version scheme, including:
  - Number of elements
  - Numbers of digits used for each element
  - Format of separators used between elements
  - Character set used for each element (consisting of alphabetic, numeric, and/or alphanumeric characters)
- The hierarchy of the elements
- Definition of what each element represents in the version scheme
- Type of change: High, Low, Admin

B.2 Version Number Usage

All changes to a given Validated Payment Software product or application must result in a new Payment Software version number. However, whether this affects the version number listed on the Website depends on the nature of the change and the Vendor's published versioning methodology. All changes that impact security functionality and/or any Secure Software Requirement must result in a change to the version number listed on the Website; use of wildcards is not permitted on the List of Validated Payment Software.

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

- Types of changes made to the Payment Software—e.g., major release, minor release, maintenance release, etc.
- Changes that have no impact on the functionality of the Payment Software or its dependencies
- Changes that have an impact on the Payment Software functionality but no impact on security or any Secure Software Requirement
- Changes that impact any security functionality or any Secure Software Requirement

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

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

Any version number that is accessible to customers and integrator/resellers must be consistent with the versioning methodology described in the Payment Software implementation guidance.

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

Appendix C: Secure Software Change Impact

Administrative and Low Impact changes to Validated Payment Software must be disclosed in this *Secure Software Change Impact* document. Note that all High Impact changes require a full Secure Software Assessment.

Secure Software Assessors or Secure SLC Qualified Vendors must complete each section of this document, and all required documents based on the type of change (see "Required Documents" section below). The Secure Software Assessor or Secure SLC Qualified Vendor is required to submit this *Secure Software Change Impact* along with supporting documentation to PCI SSC for review.

Always refer to the *Secure Software Program Guide* for information on Payment Software changes.

Payment Software Details			
Name of Payment Software		Payment Software Version	
PCI Secure Software Standard Version		Validated Listing Reference #	
Submission Date			
Type of Change (please check)	☐ Administrative	☐ Low Impact (Delta)	☐ High Impact

Payment Software Vendor Contact Information			
Vendor Name			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	
Secure Software Assessor Company Contact Information			
Secure Software Assessor Company Name			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	

Secure Software Assessor Company QA Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	

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

Required Documents (indicated with an "x")						
Type of Change	**Security Guidance**	**Attestation of Validation (AOV)**	**Secure Software Change Impact**	**Red-lined ROV**	**Report on Validation (ROV)**	**Vendor Release Agreement (VRA)**
Administrative Change	*	X	X			*
Low Impact Change	X	X	X	X		
High Impact Change	X	X	X		X	*

** If applicable*

Change Impact Details

For **each** change, provide the following information. Any change that impacts Secure Software Requirements must be reflected in the redline version of the ROV submitted. Use additional pages if needed.

Indicate which Secure Software Requirements are impacted by the change:											
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6	☐ 7	☐ 8	☐ 9	☐ 10	☐ 11	☐ 12

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

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