Security Standards Council®

Payment Card Industry (PCI)

Software Security Framework

Secure Software Lifecycle Program Guide

Version 1.1

February 2021

Document Changes

Date	Version	Description
June 2019	1.0	Initial release.
February 2021	1.1	Edits required to support the expansion of the Secure SLC Program and errata updates to clarify language and align terminology across SSF Program documents.

Table of Contents

1 Introduction 3

1.1 Related Publications 3

1.2 Updates to Documents and Security Requirements 4

2 Secure SLC Program Overview 5

3 Roles and Responsibilities 6

3.1 Vendors 6

3.2 PCI Security Standards Council 6

3.3 Secure SLC Assessor Companies 7

3.4 Third-Party Service Providers 8

4 Preparation for Assessment 9

4.1 Recommended Activities Prior to the Review 9

4.2 Required Documentation and Materials 9

4.3 Secure SLC Assessment Timeframes 10

4.4 Vendor Release Agreement (VRA) 10

4.5 Secure SLC Assessment Related Fees 11

4.5.1 Secure SLC Assessor Company Fees 11

4.5.2 Secure SLC Qualified Vendor Listing Fee 11

5 Secure SLC Assessment and Listing Process 12

6 Maintaining Secure SLC Qualified Vendor Status 14

6.1 Annual Attestation 14

6.2 Vendor Re-Assessment 15

6.3 Changes to Secure SLC Qualified Vendor Listings 17

6.3.1 Administrative Changes for Secure SLC Qualified Vendor Listings 18

6.3.2 Designated Changes for Secure SLC Qualified Vendor Listings 18

6.3.3 Maintenance Documentation Summary List 19

6.4 Listing Maintenance Fees 19

6.5 Notification Following a Security Breach, Compromise, or Known or Suspected Vulnerability 20

7 Secure SLC Assessment Reporting Considerations 21

7.1 Secure SLC Report Acceptance Process Overview 21

7.2 Delivery of the ROC and Related Materials 22

7.2.1 Access to the Portal 22

7.2.2 Listing Information 22

7.2.3 Assessor Quality Management Program 22

7.2.4 ROC Submission Reviews 23

7.2.5 Secure SLC Assessor Quality Audit 23

7.2.6 Secure SLC Assessor Company Status 24

Appendix A Elements for the List of Secure SLC Qualified Vendors 26
A.1 Secure SLC Qualified Vendor, Business Unit(s) and Location(s) 26
A.2 Validation Notes 26
A.3 Product Category 26
A.4 Secure SLC Qualification Date 27
A.5 Annual Attestation Date 27
A.6 Re-Assessment Date 27
A.7 Secure SLC Assessor Company 27
Appendix B Secure SLC Change Impact Template 28
Part 1. Secure SLC Qualified Vendor Listing Details, Contact Information and Change Type28
Part 2. Details for Administrative Change (if indicated at Part 1) 28
Part 3. Details for Designated Change (if indicated at Part 1) 29

1 Introduction

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

The PCI Secure SLC 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 SLC Assessments under the Program ("Secure SLC Assessor Companies"), and their employees who are qualified by PCI SSC to perform such Assessments ("Secure SLC Assessors").

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

***Definitions**: For purposes of this document (including Section A.3 of Appendix A hereto):*

"Eligible Software" means any software or software component that may be present in a payment environment and either (a) is directly involved in storing, processing, or transmitting payment data ("Payment Software") or (b) does not directly handle payment data but may share resources defined within a payment environment; and "Assessor" refers to either a Secure SLC Assessor Company or Secure SLC Assessor, as the context requires.

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

1.1 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 Website:

Document Name	Description
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 Compliance Reporting Template for Secure SLC Standard ("ROC Report Template")	The template document provided by PCI SSC and required to be used by Assessors to prepare PCI Secure SLC Standard Reports on Compliance. The ROC Report Template includes details on how to document the findings of a Secure SLC Assessment.
Secure SLC Attestation of Compliance ("Secure SLC AOC")	A template document provided by PCI SSC and required to be used by Secure SLC Qualified Vendors to attest to the results of their Secure SLC Assessments.

Document Name	Description
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 a Secure SLC Qualified Vendor participates in the Program.
PCI SSC Programs Fee Schedule	The current lists of PCI SSC Program fees for specific qualifications, tests, retests, training, and other services available at: https://www.pcisecuritystandards.org/program_training_and_qualification/fees
Secure SLC Assessor Feedback Form	Template document made available by PCI SSC and required to be provided by Assessors to their Vendor customers to solicit feedback regarding such Assessors and their Assessment process.

1.2 Updates to Documents and Security Requirements

This Program Guide is expected to change as necessary to align with updates to the PCI Secure SLC 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, or other requirements at any time.

2 Secure SLC Program Overview

At a high level, this Program Guide addresses the following:

- Roles and responsibilities of the primary stakeholders participating in the Secure SLC Program;
- Processes for Vendors wanting to validate against the PCI Secure SLC Standard and to manage and maintain Secure SLC Qualified Vendor status once obtained;
- Processes for Secure SLC Assessor Companies to assess candidate Secure SLC Qualified Vendors and their secure software development lifecycle processes, procedures, and practices for compliance with the PCI Secure SLC Standard;
- Quality assurance processes for Secure SLC Assessor Companies.

Vendors that are successfully validated against the PCI Secure SLC Standard for Program purposes ("Secure SLC Qualified Vendors") have demonstrated to the applicable Assessor their validated secure software development life cycle processes, procedures and practices are in compliance with the PCI Secure SLC Standard. Secure SLC Qualified Vendors are then listed on PCI SSC's list of Secure SLC Qualified Vendors on the Website (the "List of Secure SLC Qualified Vendors" or "List").

Although not required for Secure SLC Qualification, Secure SLC Qualified Vendors may also seek to have eligible software products validated to the PCI Secure Software Program.

Secure SLC Qualified Vendors with software listed on the PCI SSC List of Validated Payment Software are authorized to perform certain types of "Delta Assessments" (See *Payment Card Industry (PCI) Software Security Framework Secure Software Program Guide* on the Website) of their own software products under the Program with reduced Assessor participation, where those software products (a) are listed on the PCI SSC List of Validated Payment Software that has been successfully validated against the PCI Secure Software Standard and (b) were developed and are managed under processes that are identified for that Vendor on the List of Secure SLC Qualified Vendors.

See the PCI Secure Software Program Guide on the Website for more information about managing listed software products.

Note*: The PCI Secure SLC Standard is one of many separate and independent standards published by PCI SSC (each a "PCI SSC Standard"), such as the PCI DSS. Validation to the PCI Secure SLC Standard does not imply compliance with, or result in validation to, any other PCI SSC Standard, including but not limited to the PCI DSS.*

3 Roles and Responsibilities

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

3.1 Vendors

Vendors are responsible for:

- Selecting a Secure SLC Assessor Company to perform the initial Assessment and re-qualification Assessments every three years of the Vendor's secure software lifecycle management ("Secure SLC") processes against the PCI Secure SLC Standard;
- Ensuring policies and processes that govern how the Vendor manages and supports its Secure SLC processes for software are in place and followed consistently;
- Ensuring all tools, technologies, and techniques used to support and manage the Secure SLC are properly managed to ensure continued effectiveness;
- Managing personnel involved in the design and development of the software throughout its lifecycle, including applicable Vendor personnel and third-party contributors;
- Complying with the *Vendor Release Agreement* (VRA), including the adoption and implementation of Vulnerability Handling Policies consistent with industry best practices;
- Submitting their Secure SLC methodology, policies, procedures and supporting documentation to the Secure SLC Assessor Company for review. Per the VRA, Vendors authorize the Secure SLC Assessor Company to submit resulting reports and related information to PCI SSC;
- Paying all invoices from PCI SSC in a timely fashion;
- Maintaining an internal quality assurance process for their self-testing and attestation efforts; and
- Staying up to date with PCI Secure SLC Standard, Secure SLC Program documents, statements and guidance on the Website, as well as industry trends and best practices.

3.2 PCI Security Standards Council

PCI SSC is the standards body that maintains the PCI SSC Standards. In relation to the Secure SLC Program, PCI SSC is responsible for:

- Maintaining the list of Secure SLC Qualified Vendors on the Website;
- Maintaining the lists of Secure SLC Assessor Companies and Secure SLC Assessors on the Website;
- Providing training for and qualifying Secure SLC Assessor Companies and Secure SLC Assessors to perform Secure SLC Assessments;
- Maintaining and updating the PCI Secure SLC Standard and related documentation according to a standards lifecycle management process; and
- Reviewing all submissions to be provided to PCI SSC as part of the Program, such as Vendor applications, qualification and re-assessment materials, Reports on Compliance (ROCs) and related change submissions for compliance with baseline quality standards, including but not limited to confirming:
  - Submissions are correct as to form;

- Secure SLC Assessor Companies properly determine whether Vendors are eligible for qualification under the Secure SLC Program (PCI SSC reserves the right to remove from the list of Secure SLC Qualified Vendors on the Website any Secure SLC Qualified Vendor or reject any candidate Secure SLC Qualified Vendor determined to be ineligible for the Program);
- Secure SLC Assessor Companies adequately report Secure SLC compliance of Vendors in their associated submissions; and
- Detail provided in the submissions meets PCI SSC reporting requirements.

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

Note*: PCI SSC does not perform Assessments of or validate Vendors. Assessment and validation is the role of the Secure SLC Assessor Company and its Secure SLC Assessors. Vendor listing on the List of Secure SLC Qualified Vendors signifies that the applicable Secure SLC Assessor Company has determined that the Vendor complies with the PCI Secure SLC Standard, that the Secure SLC Assessor Company has submitted a corresponding ROC to PCI SSC, and that PCI SSC has determined that such ROC has satisfied all PCI SSC documentation requirements as of the time of PCI SSC's review.*

3.3 Secure SLC Assessor Companies

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

Note*: Subject to satisfaction of all applicable requirements, a SSF Assessor Company may participate in one or more PCI SSC programs associated with the SSF. The PCI SSC programs for which a SSF Assessor Company is a qualified by PCI SSC are specified in the SSF Assessor Company listing on the Website.*

- Ensuring that the Secure SLC Assessor Company and its Secure SLC Assessors remain in good standing for Program purposes;
- Ensuring that its Secure SLC Assessors each complete all required Secure SLC Assessor training:
- Performing Secure SLC Assessments in accordance with the PCI Secure SLC Standard, this Program Guide, the *SSF Qualification Requirements* and the SSF Agreement;
- Providing an opinion regarding whether the Secure SLC Assessor Company's Vendor customer meets the intent and requirements of the PCI Secure SLC Standard;
- Documenting each Secure SLC Assessment in a ROC and accompanying Attestation of Compliance ("AOC") using the Secure SLC ROC Report and AOC Templates;
- Providing documentation within each ROC and accompanying AOC to demonstrate the Vendor's compliance with the PCI Secure SLC Standard;
- Submitting each ROC to PCI SSC, along with the VRA, if applicable, each signed by both Secure SLC Assessor Company and Vendor;
- Maintaining an internal quality assurance process for their Secure SLC Assessment efforts;

- Staying up to date with PCI SSC statements and guidance, industry trends, and best practices; and
- Satisfying all applicable SSF and Program requirements at all times, including but not limited to successful completion of annual requalification and adhering to the applicable *SSF Qualification Requirements*.

It is the Secure SLC Assessor Company's responsibility to assess a Vendor's Secure SLC processes for compliance with the PCI Secure SLC Standard and document its findings and opinions in the applicable ROC using the applicable ROC report template. PCI SSC does not approve ROCs from a technical perspective; it performs quality assurance reviews to confirm that the ROC adequately documents the Assessor's validation and attestation of compliance.

3.4 Third-Party Service Providers

A Vendor's Secure SLC process may require or utilize one or more products or services provided by third-parties (e.g., unrelated companies that perform software development services, code reviews, testing of software, and/or other services). Such third-parties are considered "Third-Party Service Providers" with respect to the Vendor's Secure SLC processes, and their products and services, to the extent required, utilized, or incorporated for, into or as part of the Vendor's Secure SLC processes, are evaluated/assessed as part of Vendor's Secure SLC Assessment. If eligible, a Third-Party Service Provider may choose to undergo its own Secure SLC Assessment for its own applicable product(s) or service(s).

***Note**: For a given Secure SLC Assessment, the supporting Third-Party Service Provider product(s) or service(s) are considered part of the Vendor's overall Secure SLC processes, are evaluated/assessed as part of the Vendor's entire secure software lifecycle process Assessment and are not eligible for separate listing as part of the Secure SLC Program.*

4 Preparation for Assessment

4.1 Recommended Activities Prior to the Review

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

- Review the PCI Secure SLC Standard and related documentation located on the Website;
- Determine/assess readiness to comply with the PCI Secure SLC Standard:
  - Perform a gap analysis between the Secure SLC methods, policies, procedures, practices, etc. to be assessed and the requirements of the PCI Secure SLC Standard;
  - Correct any gaps; and
  - If desired, the Vendor can engage the Secure SLC Assessor Company to perform a pre-assessment or gap analysis of the Vendor's software lifecycle practices. If the Assessor notes deficiencies that would prevent a compliant result, the Assessor may provide the candidate with a list of items to be addressed before the formal Assessment begins.

4.2 Required Documentation and Materials

All PCI SSC published information relevant to the PCI Secure SLC Standard and Program is available on the Website.

In connection with each Assessment, the Vendor must provide the applicable supporting documentation to the Secure SLC Assessor Company. Examples of documentation and other items the Vendor should be prepared to submit to the Secure SLC Assessor Company include, but are not limited to:

***Note**: The Secure SLC Assessor Company may request additional material as necessary (no Vendor documentation supporting the assessment is sent directly to PCI SSC).*

- Documentation including policies and processes, internal standards, requirement mappings, internal presentations, training materials, or any other documentation or records that clearly and consistently illustrate that the Vendor has made reasonable efforts to understand and monitor its external security and compliance requirements;
- Software-specific documentation, features lists, software-specific security control inventories, change-management documentation, risk assessment reports, penetration test results, output from active monitoring systems, bug bounty program data, or any other evidence or information that clearly and consistently illustrates that the effectiveness of software security controls is monitored and that software-specific software security controls are updated, augmented, or replaced when no longer effective at satisfying their intended purpose of resisting attacks;
- Documentation supporting software communications such as release notes to communicate all software changes to stakeholders upon software updates, publicly available information or notifications regarding the software updates, and change summary information for software updates;
- Additional documentation—such as diagrams and flowcharts—that will aid in the Secure SLC review; and

- The Vendor's executed VRA (if PCI SSC does not already have a copy of the then most current version of the VRA signed by the Vendor).

4.3 Secure SLC Assessment Timeframes

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

- Whether the Vendor's Secure SLC processes and procedures meet all requirements of the PCI Secure SLC Standard at the start of the Assessment
  - Corrections to the Vendor's Secure SLC processes to achieve compliance will delay validation.
- Prompt payment of the fee due to PCI SSC
  - PCI SSC will not commence review of the ROC until the applicable fee has been paid.
- Quality of the Secure SLC Assessor Company's submission to PCI SSC
  - Incomplete submissions or those containing errors, for example, missing or unsigned documents, incomplete, inconsistent, or insufficient submissions, will result in delays in the review process.
  - If the quality of the submission results in PCI SSC reviewing the ROC more than once, providing comments back to the Secure SLC Assessor Company to address each time, this will increase the length of time for the review process.

Any Assessment timeframes provided by a Secure SLC Assessor Company should be considered estimates. Problems found during the review or acceptance process, discussions required between the Secure SLC Assessor, the Vendor, and/or PCI SSC, or other matters may significantly impact review times and cause delays and/or cause the review to end prematurely.

4.4 Vendor Release Agreement (VRA)

The Vendor's signed copy of the then most current version of the *Vendor Release Agreement* (available on the Website) must be provided to the Secure SLC Assessor Company at the beginning of each Secure SLC Assessment. The Secure SLC Assessor Company provides the VRA to PCI SSC with the ROC and AOC submitted for that Assessment. Among other things, the VRA covers confidentiality issues, the Vendor's agreement to adhere to Secure SLC Program requirements, policies and procedures, and gives permission to the Vendor's Secure SLC Assessor Company to release ROCs 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 ROC will **not** be reviewed by PCI SSC without the then most 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 ROC for the same Vendor.*

4.5 Secure SLC Assessment Related Fees

4.5.1 Secure SLC Assessor Company Fees

The prices and fees charged by Secure SLC Assessor Companies are not set by PCI SSC. These fees are negotiated between the Secure SLC Assessor Company and its customers (i.e., Vendors seeking Secure SLC assessments to become Secure SLC Qualified Vendors). Before deciding on a Secure SLC Assessor Company, it is recommended that the Vendor check the list of Secure SLC Assessor Companies on the Website, talk to several Secure SLC Assessor Companies and follow its own vendor-selection processes.

4.5.2 Secure SLC Qualified Vendor Listing Fee

Vendors are required to pay a Secure SLC Qualified Vendor Listing Fee to PCI SSC. The New Secure SLC Qualified Vendor Listing Fee will be invoiced and must be received by PCI SSC before the applicable Secure SLC Assessment ROC submission will be reviewed, accepted and added to the List of Secure SLC Qualified Vendors by PCI SSC. Upon Acceptance of the Secure SLC Assessment ROC submission by PCI SSC, PCI SSC will sign and return a copy of the Attestation of Compliance to both the Vendor and the Secure SLC Assessor Company.

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

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

PCI SSC will bill the Vendor for the New Secure SLC Vendor Listing Fee—the Vendor pays this fee directly to PCI SSC.

5 Secure SLC Assessment and Listing Process

Secure SLC Assessments are performed by Secure SLC Assessor Companies and involve a detailed analysis of the Vendor's secure SLC processes to validate whether the Vendor meets the requirements of the PCI Secure SLC Standard.The following is a high-level overview of the process for initiating and completing a Secure SLC Assessment:

- Vendor initiates the process by selecting a Secure SLC Assessor Company from the Website and negotiates any costs and agreements necessary to perform the Assessment with the Secure SLC Assessor Company.
- The Vendor and Secure SLC Assessor Company determine the scope of the Assessment.
- The Secure SLC Assessor Company assesses the Vendor's secure SLC processes, including planning, development, testing, implementation, maintenance, patching, etc. to determine whether the Vendor meets the requirements of the PCI Secure SLC Standard.
- If the Secure SLC Assessor Company determines that the Vendor's secure SLC processes satisfy all applicable requirements, it prepares a corresponding Secure SLC Report on Compliance (ROC) including all test results, opinions, and conclusions along with an Attestation of Compliance (AOC), and submits them to PCI SSC for review.
- PCI SSC issues an invoice to the Vendor for review of the submission.
- Once PCI SSC receives full payment of the invoice from the Vendor, review of the submission will commence. For detailed information regarding this part of the process, refer to Section 7.1, Secure SLC Report Acceptance Process Overview.
- Upon and subject to successful completion of the submission review, and final acceptance and approval of the ROC by PCI SSC ("Acceptance"), PCI SSC will:
  - Add a listing identifying the Vendor to the List of Secure SLC Qualified Vendors on the Website (each a "Listing");
  - Countersign the AOC and send a copy to the Vendor and the Secure SLC Assessor Company.
- Each Listing is valid for a period of three years if the Vendor continues to meet all Secure SLC Program requirements and remains in good standing.

The Secure SLC Assessment and Listing Process is illustrated in Figure 1.

Figure 1. Secure SLC Assessment and Listing Process

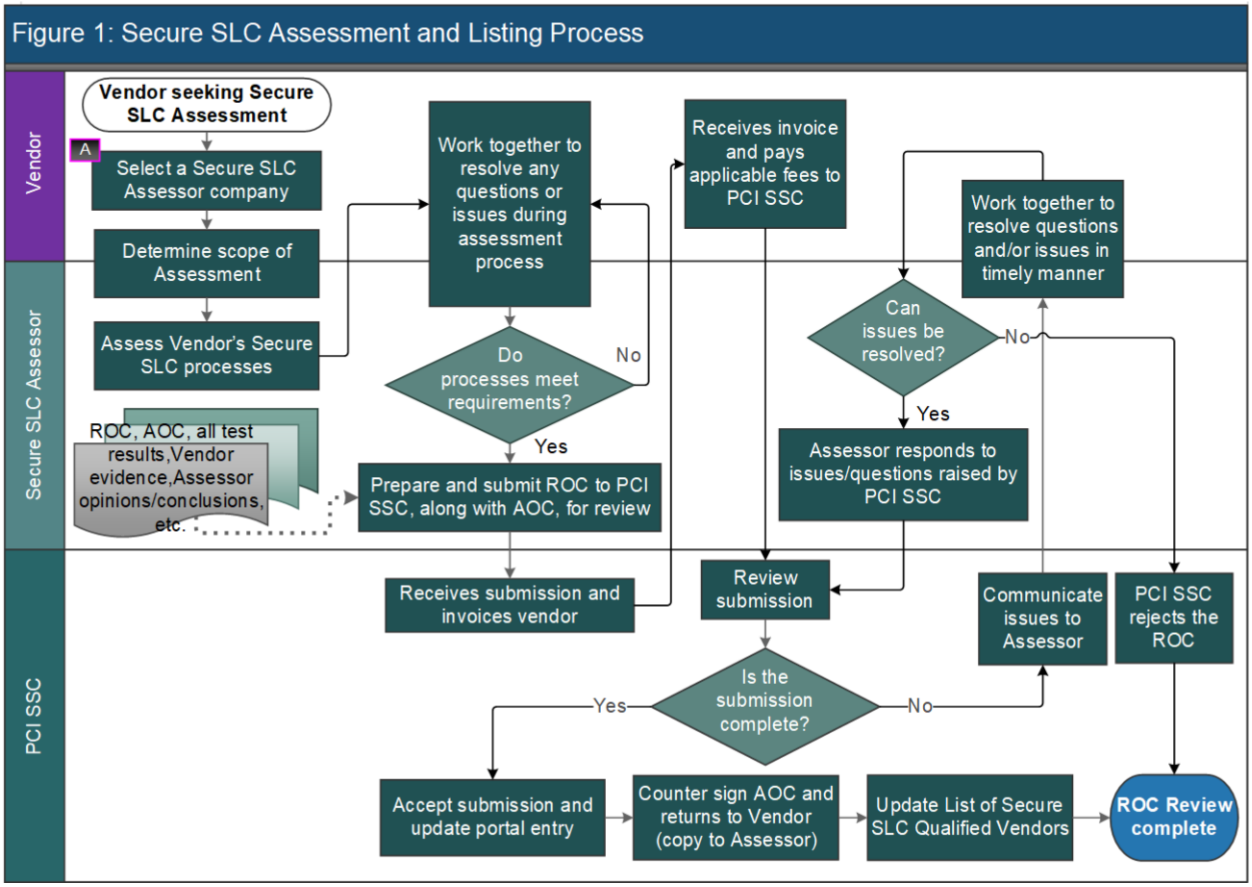
Figure 1: Secure SLC Assessment and Listing Process
Vendor
Secure SLC Assessor
PCI SSC
Vendor seeking Secure SLC Assessment
A
Select a Secure SLC Assessor company
Determine scope of Assessment
Assess Vendor's Secure SLC processes
ROC, AOC, all test results,Vendor evidence,Assessor opinions/conclusions, etc.
Work together to resolve any questions or issues during assessment process
Do processes meet requirements?
No
Yes
Prepare and submit ROC to PCI SSC, along with AOC, for review
Receives submission and invoices vendor
Receives invoice and pays applicable fees to PCI SSC
Review submission
Is the submission complete?
Yes
No
Accept submission and update portal entry
Counter sign AOC and returns to Vendor (copy to Assessor)
Update List of Secure SLC Qualified Vendors
ROC Review complete
Work together to resolve questions and/or issues in timely manner
Can issues be resolved?
No
Yes
Assessor responds to issues/questions raised by PCI SSC
Communicate issues to Assessor
PCI SSC rejects the ROC

6 Maintaining Secure SLC Qualified Vendor Status

Following the Assessment, submittal of all applicable materials and fees, PCI SSC review and Acceptance, the Vendor will be designated a Secure SLC Qualified Vendor and listed on the Website. The applicable Listing will remain current for a period of three years from the date that the Secure SLC Qualified Vendor was first accepted and approved by PCI SSC ("Accepted"), as long as the Vendor continues to meet all Secure SLC Program requirements and remains in good standing as a Secure SLC Qualified Vendor.

***Note**: PCI SSC reserves the right to withdraw Acceptance as indicated in Section 6.5 if a suspected vulnerability/ security issue takes place.*

6.1 Annual Attestation

Annually, the Secure SLC Qualified Vendor is required to submit an updated *Attestation of Compliance* (AOC) to PCI SSC, performing the Annual Attestation steps. PCI SSC will typically provide a courtesy reminder via e-mail to the Secure SLC Qualified Vendor's Primary Contact 90 calendar days prior to the due date of each attestation, but it is the sole responsibility of the Secure SLC Qualified Vendor to comply with annual attestation requirements and maintain its Listing, regardless of such courtesy reminder(s).

As part of this annual process, Secure SLC Qualified Vendors are required to confirm:

- Whether any changes have been made to its Secure SLC processes (including but not limited to policies, procedures, testing methodologies, capabilities, etc.) and, if so, document all changes that have been made to those processes; and
  - That its validated Secure SLC processes continue to meet the PCI Secure SLC Standard; and
  - That changes made to its Secure SLC processes do not impact compliance with any of the then current requirements of the Program or Secure SLC Standard; and
  - That PCI SSC has been advised of all changes made to the Secure SLC Qualified Vendor's software lifecycle process that necessitate a change to the Vendor's listing on the Website.
- The Secure SLC Qualified Vendor is required to consider the impact of external threats and whether updates to its Secure SLC processes are necessary to address changes to the external threat environment.
- The updated AOC and any applicable documentation are submitted by the Secure SLC Qualified Vendor to the PCI SSC Secure SLC Program Manager. An updated AOC must be submitted to PCI SSC ahead of the annual attestation date. PCI SSC will typically review and respond regarding such submittals within 30 days. If PCI SSC does not receive the submittal prior to the annual attestation date, the Secure SLC Qualified Vendor's Listing will be subject to early administrative expiry, as follows:
  - Fourteen (14) calendar days following the annual attestation date, the corresponding Listing will be updated to show the Listing's annual attestation

***Note**: To avoid early administrative expiry (described below), Vendors should begin the annual attestation process in advance of their annual attestation date.*

date in **Orange** for a period of 90 consecutive calendar days past the annual attestation date.

- If the updated and complete AOC is received by PCI SSC within this 90-day period, PCI SSC will update the corresponding Listing's annual attestation date with the new date and remove the **Orange** status.
- If the updated and complete AOC is not received by PCI SSC within this 90-day period, the Secure SLC Listing's annual attestation date will be updated to show the date in **Red**.
- Once in **Red**, a full Assessment (including applicable fees) is required to return the Secure SLC Qualified Vendor Listing status to good standing.

***Note:** Annual attestation submissions received more than 30 calendar days past the annual attestation date will be assessed a late fee (Secure SLC Qualified Vendor Annual Attestation Late Fee, as listed in the PCI SSC Programs Fee Schedule).*

PCI SSC will, upon receipt of the updated Attestation of Compliance: (i) review the submission for completeness; and (ii) sign and return a copy of the updated Attestation of Compliance to the Secure SLC Qualified Vendor.

The process flow for Vendor Annual Attestation is illustrated in Figure 2a.

6.2 Vendor Re-Assessment

As a Secure SLC Qualified Vendor Listing approaches its 3-year re-assessment date, PCI SSC will notify the Vendor of the pending re-assessment. The two options available for Vendor consideration are either a new full Assessment or expiry:

New Full Assessment: If the Vendor wishes to remain on the List of Secure SLC Qualified Vendors, the Vendor must engage a Secure SLC Assessor Company to perform a new full Assessment against the then-current version of the PCI Secure SLC Standard, resulting in a new Acceptance on or before the re-assessment date. This new full Assessment must follow the same process as an initial Secure SLC Qualified Vendor Assessment.

Expiry: List of Secure SLC Qualified Vendors for which a new Acceptance has not occurred on or before the applicable re-assessment date will appear in **Orange** for the first 90 calendar days past re-assessment, and in **Red** thereafter.

***Note**: If a Vendor fails to meet the requirements of a full Assessment, its Secure SLC Qualified Vendor status is revoked, and the Vendor's Listing will be removed from the Website.*

The process flow for Vendor Re-Assessment is illustrated in Figure 2b.

Figure 2a & 2b. Secure SLC Qualified Vendor Annual Attestation and Re-Assessment

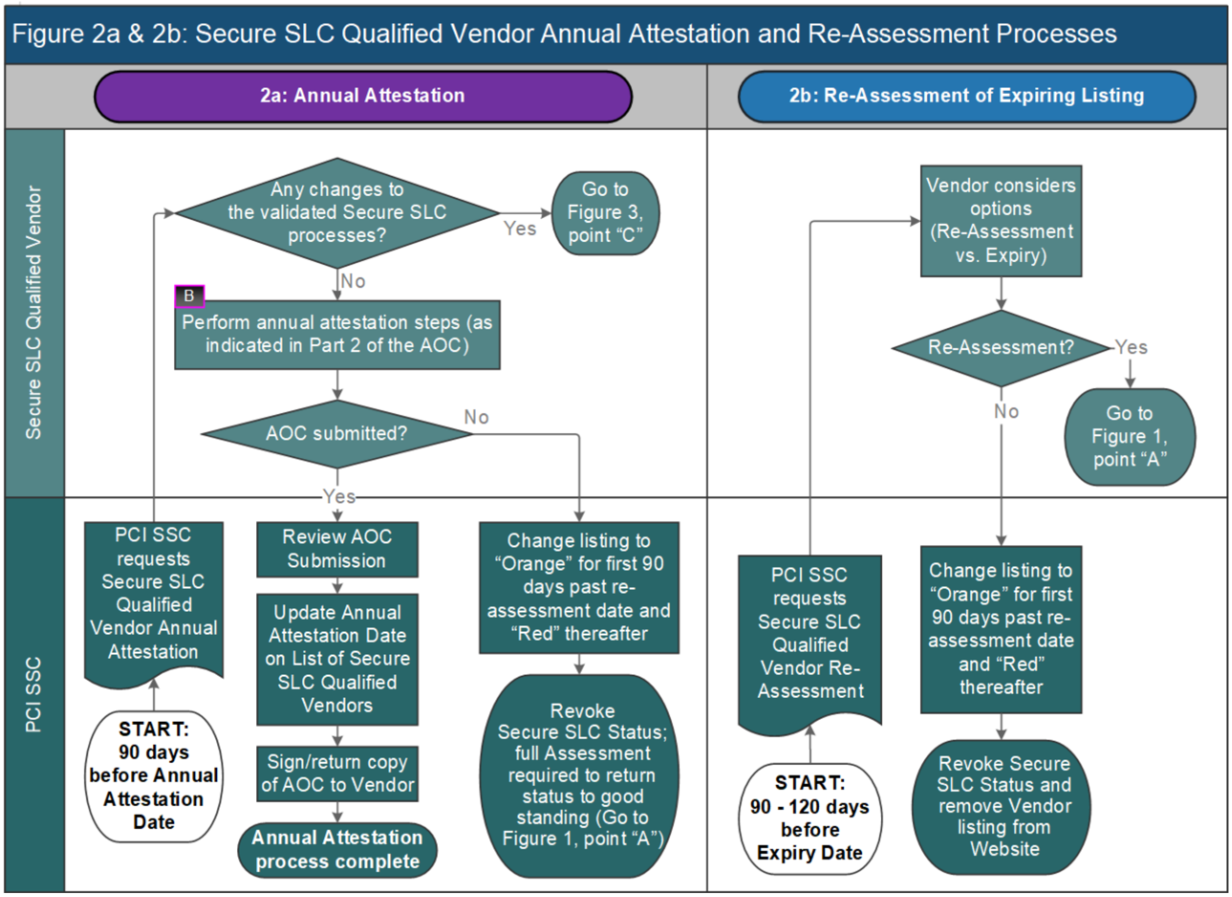
Figure 2a & 2b: Secure SLC Qualified Vendor Annual Attestation and Re-Assessment Processes
2a: Annual Attestation
2b: Re-Assessment of Expiring Listing
Secure SLC Qualified Vendor
PCI SSC
Any changes to the validated Secure SLC processes?
Yes
Go to Figure 3, point "C"
No
B
Perform annual attestation steps (as indicated in Part 2 of the AOC)
AOC submitted?
No
Yes
PCI SSC requests Secure SLC Qualified Vendor Annual Attestation
START: 90 days before Annual Attestation Date
Review AOC Submission
Update Annual Attestation Date on List of Secure SLC Qualified Vendors
Sign/return copy of AOC to Vendor
Annual Attestation process complete
Change listing to "Orange" for first 90 days past re-assessment date and "Red" thereafter
Revoke Secure SLC Status; full Assessment required to return status to good standing (Go to Figure 1, point "A")
Vendor considers options (Re-Assessment vs. Expiry)
Re-Assessment?
Yes
Go to Figure 1, point "A"
No
PCI SSC requests Secure SLC Qualified Vendor Re-Assessment
START: 90 - 120 days before Expiry Date
Change listing to "Orange" for first 90 days past re-assessment date and "Red" thereafter
Revoke Secure SLC Status and remove Vendor listing from Website

6.3 Changes to Secure SLC Qualified Vendor Listings

Vendors may update their Listings for various reasons. Changes do not have any impact on Listing re-assessment dates or annual attestation dates. Changes to Listings are categorized as follows:

Table 1. Changes to Secure SLC Qualified Vendor Listing

Change Type	Description
Administrative	Changes made to a listed Vendor that have no impact on the Vendor's compliance with the *PCI Secure SLC Standard*, but where the Listing of Secure SLC Qualified Vendors is updated to reflect the change. Examples of administrative changes include, but are not limited to, corporate identity changes and changes to Listing details. See Section 6.3.1, Administrative Changes for Secure SLC Qualified Vendor Listings for details.
Designated	Designated Changes are for changes to the Vendor's Listing that are limited to: Add or remove a Product Category used in Secure SLC development See Section 6.3.2, Designated Changes for Secure SLC Qualified Vendor Listings for details.

The process flow for Updates to Secure SLC Qualified Vendor Listings is illustrated in Figure 3.

Figure 3. Updates to Secure SLC Qualified Vendor Listings

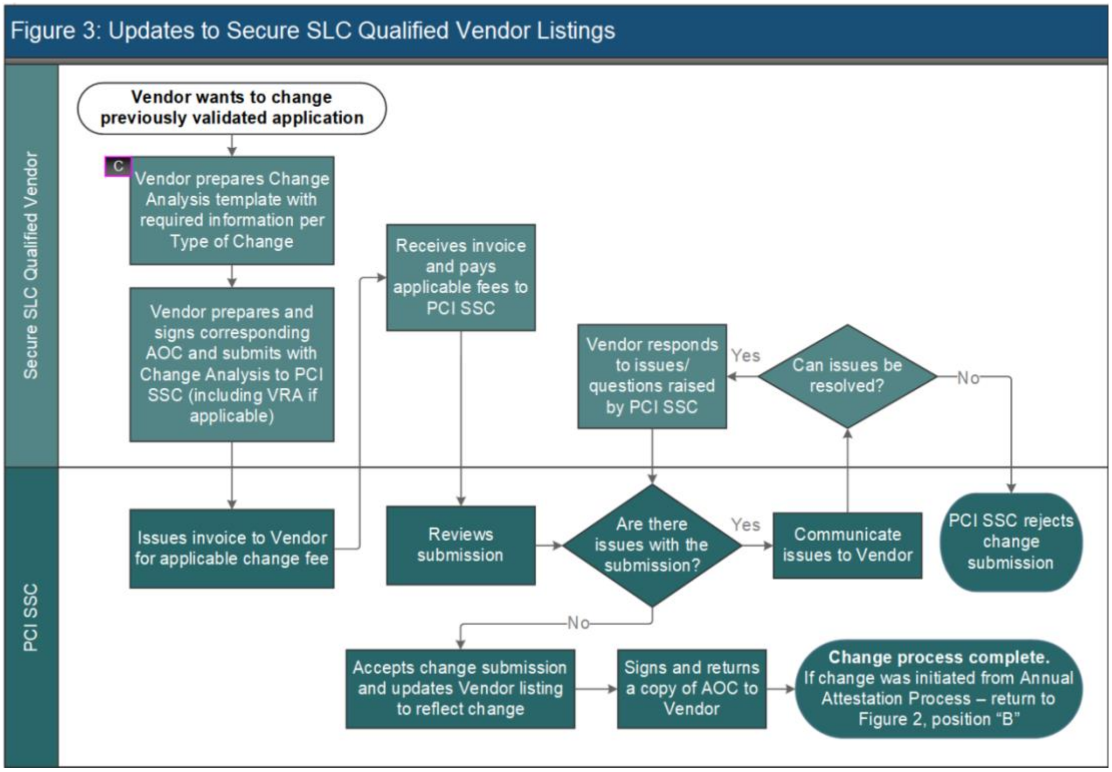
Figure 3: Updates to Secure SLC Qualified Vendor Listings
Secure SLC Qualified Vendor
PCI SSC
Vendor wants to change previously validated application
C
Vendor prepares Change Analysis template with required information per Type of Change
Vendor prepares and signs corresponding AOC and submits with Change Analysis to PCI SSC (including VRA if applicable)
Receives invoice and pays applicable fees to PCI SSC
Vendor responds to issues/ questions raised by PCI SSC
Yes
Can issues be resolved?
No
Issues invoice to Vendor for applicable change fee
Reviews submission
Are there issues with the submission?
Yes
Communicate issues to Vendor
PCI SSC rejects change submission
No
Accepts change submission and updates Vendor listing to reflect change
Signs and returns a copy of AOC to Vendor
Change process complete. If change was initiated from Annual Attestation Process – return to Figure 2, position "B"

6.3.1 Administrative Changes for Secure SLC Qualified Vendor Listings

***Note**: Administrative Changes are only permissible for Secure SLC Qualified Vendors that are then on the List and have not passed their re-assessment date.*

Administrative Changes are limited to updates where no changes to a listed Vendor's Secure SLC processes have occurred, but the Vendor wishes to request a change to the way the Vendor is currently listed on the Website. See Section 6.3.3, Maintenance Documentation Summary List for a summary of what is to be provided.

The Vendor prepares a change analysis using the *Secure SLC Change Impact Template* ("Change Impact Template") in Appendix B.

Minimum required information:

- Name and reference number of the Vendor Listing
- Description of the change
- "Type of Change" selected on template is "Administrative"

Administrative Change submission process:

- The Vendor prepares and signs the corresponding AOC (and new VRA if applicable) and sends it to the PCI SSC Software Security Framework Program Manager with the Change Impact Template.
- PCI SSC will then issue an invoice to the Vendor for the applicable change fee; and
- Upon payment of the invoice, PCI SSC will review the Administrative change submission.
- Should there be quality issues associated with any aspect of the submission, PCI SSC will provide these details to the Vendor and work with them to resolve.
  - PCI SSC reserves the right to reject any change submission 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.
- Following successful PCI SSC review of the change, PCI SSC will:
  - Update the Vendor's Listing to reflect with the new information; and
  - Sign and return a copy of the corresponding AOC to the Vendor.

6.3.2 Designated Changes for Secure SLC Qualified Vendor Listings

Designated Changes are intended to keep the Vendor's Listing up to date. See Section 6.3.3, Maintenance Documentation Summary List for a summary of what is to be provided.

Designated Changes are amendments made only to a Vendor's current Listing to add or remove a category used by the Vendor in its validated and Accepted Secure SLC development lifecycle.

The Vendor prepares a change analysis using the Change Impact Template in Appendix B.

Minimum required information:

- Name and reference number of the Secure SLC Qualified Vendor
- Description of the change
- "Type of Change" selected on template is "Designated"

Designated Change submission process:

- The Vendor prepares and signs the corresponding AOC (and new VRA if applicable) and sends it to the PCI SSC Software Security Framework Program Manager with the Change Impact Template.
- PCI SSC will then issue an invoice to the Vendor for the applicable change fee; and
- Upon payment of the invoice, PCI SSC will review the Designated Change submission.
- Should there be quality issues associated with any aspect of the submission, PCI SSC will communicate them to the Vendor.
  - PCI SSC reserves the right to reject any change submission if it determines that a change described therein and purported to be a Designated Change by the Vendor is ineligible for treatment as a Designated Change.
- Following successful PCI SSC review of the change, PCI SSC will:
  - Update the Vendor's Listing to reflect the new information; and
  - Sign and return a copy of the corresponding AOC to the Vendor.

6.3.3 Maintenance Documentation Summary List

Administrative Change	Designated Change	Annual Attestation
• Attestation of Compliance (AOC) • Change Impact Template** • New VRA* • Fee	• Attestation of Compliance (AOC) • Change Impact Template** • New VRA* • Fee	• Attestation of Compliance (AOC) • New VRA*

* *If applicable.*

*** The Change Impact Template in Appendix B is mandatory for the Vendor when submitting Administrative and Designated Changes to PCI SSC.*

6.4 Listing Maintenance Fees

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

For any change affecting the Listing of a Secure SLC Qualified Vendor, the applicable fee will be invoiced and must be received by PCI SSC for the changes to be reviewed, Accepted, and added to the List of Secure SLC Qualified Vendors.

Upon Acceptance, PCI SSC will sign and return a copy of the AOC to the Vendor.

There is no PCI SSC fee associated with the processing of annual attestations.

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

***Note:** PCI SSC will invoice the Vendor for all Listing Maintenance Fees, and the Vendor will pay these fees directly to PCI SSC.*

A Vendor must already be identified on the List and not yet have passed its re-assessment date to have a change Accepted and reflected on the List.

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

In the event of a Security Issue (defined in the VRA) relating to a Secure SLC Qualified Vendor, the VRA requires the Vendor to notify PCI SSC. Vendors must be aware of and adhere to their obligations under the VRA (including but not limited to obligations in the event of a Security Issue).

7 Secure SLC Assessment Reporting Considerations

7.1 Secure SLC Report Acceptance Process Overview

The Secure SLC Assessor Company performs the Secure SLC Assessment in accordance with the PCI Secure SLC Standard and produces a ROC that is shared with the Vendor. If the ROC does not have all items in place, the Vendor must address those items, and the Secure SLC Assessor Company assesses the items and updates the ROC prior to submission to PCI SSC. Once the Secure SLC Assessor Company is satisfied that all documented issues have been resolved by the Vendor, the Secure SLC Assessor Company submits the ROC and all other required materials to PCI SSC through the Portal.

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

***Note**: It is common for submissions to require several iterations before the application is Accepted. Adequate QA review of the submission as part of the Secure SLC 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. The status of submissions can be viewed within the Portal.*

PCI SSC communicates any quality issues associated with ROCs to the Secure SLC Assessor Company. PCI SSC endeavors to communicate in real time when possible. It is the responsibility of the Secure SLC 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 ROC to reflect adequate documentation to support the Secure SLC Assessor Company's decisions, whereas more extensive issues may require the Secure SLC Assessor Company to perform further testing, requiring the Secure SLC Assessor Company to notify the Vendor that re-testing is needed and to schedule that testing with the Vendor.

ROCs that have been returned to the Secure SLC 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 SLC Assessor Company must inform the PCI SSC of the timeline for response and PCI SSC may grant an extension. Lack of response by the Secure SLC Assessor Company regarding ROCs returned for correction may result in the submission being closed and the possibility of further action taken by the PCI SSC against the Secure SLC Assessor Company. Submissions that have been closed will not be reopened and must be resubmitted as new ROC submissions, including payment of invoices.

The process flows for the ROC Submittal, Review and Acceptance process are detailed in Figure 1.

7.2 Delivery of the ROC and Related Materials

All documents required in connection with the Secure SLC validation process must be submitted to PCI SSC by the Secure SLC Assessor Company through a secure submission website designated by PCI SSC (the Portal). Council staff 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 contact information, incomplete or inconsistent documentation, and inconsistent categories being insufficiently explained. Incomplete or inconsistent submissions may result in a significant delay in processing submissions and/or may not be accepted for review by the PCI SSC.

7.2.1 Access to the Portal

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

Link to Portal: https://programs.pcissc.org/

7.2.2 Listing Information

The List of Secure SLC Qualified Vendors will contain, at minimum, the information specified below. Each characteristic is detailed in Appendix A, Elements for the List of Secure SLC Qualified Vendors:

- Secure SLC Qualified Vendor
  - Business Unit
  - Location Address
  - Country
- Product Categories (specifying categories of software developed by the Vendor in accordance with the Vendor’s validated Secure SLC process
- Validation Notes (Secure SLC version)
- Secure SLC Qualified Vendor Program qualification date
- Annual Attestation
- Re-Assessment Date
- Secure SLC Assessor Company

7.2.3 Assessor Quality Management Program

Secure SLC 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 SLC Assessor Companies are described below.

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

Figure 4. Secure SLC Qualified Vendor QA Programs for Report Reviews

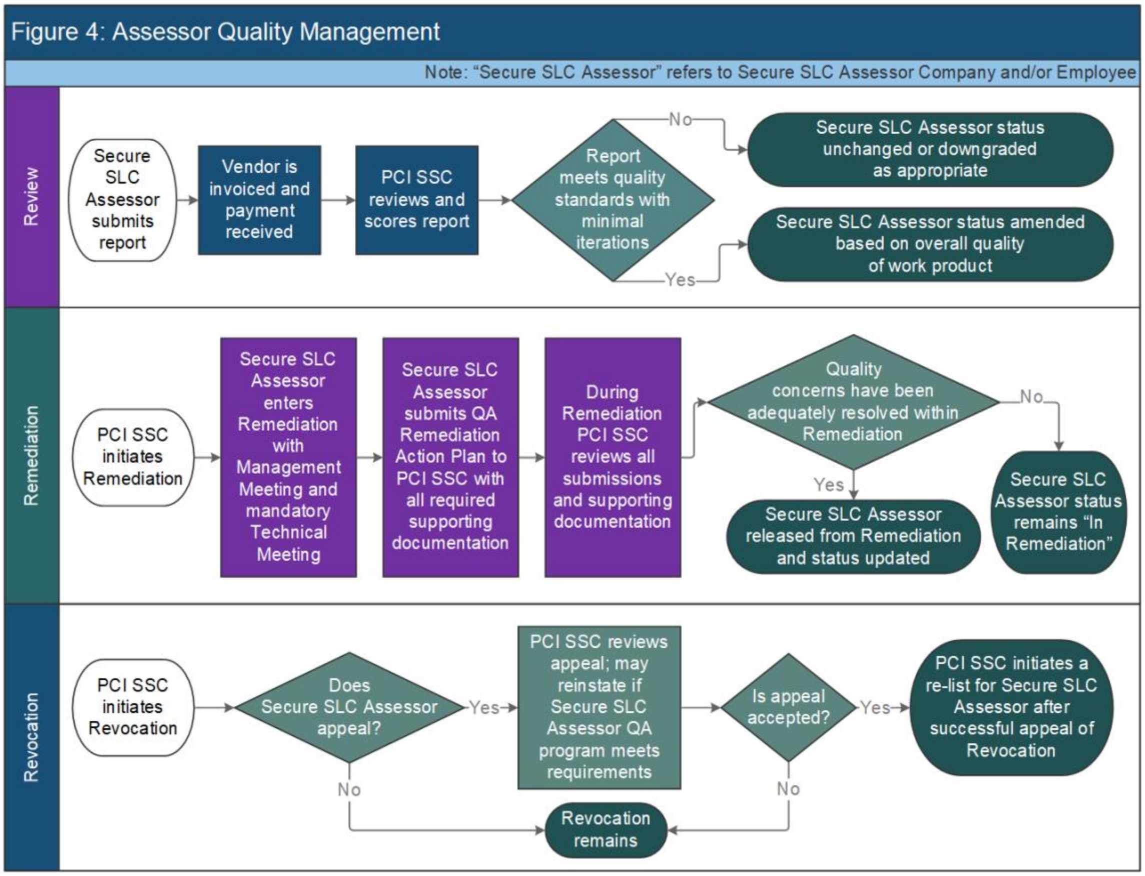
Figure 4: Assessor Quality Management
Note: "Secure SLC Assessor" refers to Secure SLC Assessor Company and/or Employee
Review
Secure SLC Assessor submits report
Vendor is invoiced and payment received
PCI SSC reviews and scores report
Report meets quality standards with minimal iterations
No
Secure SLC Assessor status unchanged or downgraded as appropriate
Yes
Secure SLC Assessor status amended based on overall quality of work product
Remediation
PCI SSC initiates Remediation
Secure SLC Assessor enters Remediation with Management Meeting and mandatory Technical Meeting
Secure SLC Assessor submits QA Remediation Action Plan to PCI SSC with all required supporting documentation
During Remediation PCI SSC reviews all submissions and supporting documentation
Quality concerns have been adequately resolved within Remediation
No
Secure SLC Assessor status remains "In Remediation"
Yes
Secure SLC Assessor released from Remediation and status updated
Revocation
PCI SSC initiates Revocation
Does Secure SLC Assessor appeal?
Yes
PCI SSC reviews appeal; may reinstate if Secure SLC Assessor QA program meets requirements
Is appeal accepted?
Yes
PCI SSC initiates a re-list for Secure SLC Assessor after successful appeal of Revocation
No
No
Revocation remains

7.2.4 ROC Submission Reviews

PCI SSC's AQM reviews each ROC 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 Vendor is determined to be eligible for qualification under the Secure SLC Program and the submission is complete, the AQM analyst will complete a full review of the ROC 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 SLC 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 SLC Assessor Company's submission to provide reasonable assurance that a quality Assessment was performed.

7.2.5 Secure SLC Assessor Quality Audit

The purpose of the Secure SLC Assessor Company audit process is to provide reasonable assurance that the Assessment of the Vendor's Secure SLC process 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 SLC Assessor Company audits are addressed in the *SSF Qualification Requirements*, and Secure SLC 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 SLC Assessor Companies to audit internal QA programs, at the expense of the Secure SLC Assessor Companies. Refer to the *SSF Qualification Requirements for* information on PCI SSC's audit process.

7.2.6 Secure SLC Assessor Company Status

The Secure SLC Program recognizes several status designations for Secure SLC Assessor Companies: "In Good Standing," "Remediation," and "Revocation." The status of a Secure SLC 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 SLC 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 SLC Assessor Company may move directly from "In Good Standing" to "Revocation."*

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

7.2.6.1 In Good Standing

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

7.2.6.2 Remediation

A Secure SLC 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 SLC 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 SLC Assessor Companies to improve performance by working closely with PCI SSC staff. Additionally, Remediation helps to assure that the baseline standard of quality for Secure SLC Assessor Companies and Secure SLC Assessors is maintained.

7.2.6.3 Revocation

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

The SSF Assessor Company may appeal Revocation, but unless otherwise approved by PCI SSC in writing in each instance, the Secure SLC Assessor Company (and its Secure SLC Assessors) is not permitted to perform Secure SLC Assessments, process ROCs, or otherwise participate in the Secure SLC Program. The Secure SLC 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.

Appendix A Elements for the List of Secure SLC Qualified Vendors

A.1 Secure SLC Qualified Vendor, Business Unit(s) and Location(s)

This entry denotes the **Vendor** for the validated SLC process.

A.2 Validation Notes

Validation Notes are used by PCI SSC to denote what standard, and the specific version thereof, was used to assess the compliance of a Secure SLC Qualified Vendor.

A.3 Product Category

Only Vendors of Payment Software and other Eligible Software may seek validation as Secure SLC Qualified Vendors (see definitions of Payment Software and Eligible Software in Section 1 of the Program Guide). The Vendor must choose the category that best describes the primary function of the software, applications or components developed using the validated Secure SLC process from the list below.

Function	Description
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.
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.
Payment Back Office	Eligible 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 SLC Assessment.
Payment Component	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. Payment software may include, but is not limited to, mobile payment applications or mobile browser payment components.
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.
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.
POS Admin	Eligible Software that administers or manages POS applications.
POS Face-to-Face/POI	Point-of-sale Payment 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.

Function	Description
POS Kiosk	Point-of-sale Payment Software for payment card transactions that occur in attended or unattended kiosks—for example, in parking lots.
POS Specialized	Point-of-sale Payment Software that can be used by merchants for specialized transmission methods, such as Bluetooth, Category 1 or 2 mobile, VOIP, etc.
POS Suite/General	Point-of-sale Payment 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.
Shopping Cart & Store Front	Payment Software for e-commerce merchants, where the consumer selects purchases from the Store Front and enters cardholder data in the Shopping Cart, then the Shopping Cart transmits and processes that cardholder data for authorization and settlement. This is different from the Web mentioned under POS Suite, where the merchant manually enters the data in a virtual POS for authorization and settlement.

A.4 Secure SLC Qualification Date

The Secure SLC Qualification Date is used by PCI SSC to indicate when the Vendor‘s initial listing occurred.

A.5 Annual Attestation Date

The Annual Attestation Date indicates the date on which the Vendor is due for its annual attestation via Attestation of Compliance. Orange- or red-colored indicators by this field signify that the Vendor is overdue for submittal to PCI SSC.

A.6 Re-Assessment Date

The Re-Assessment Date is used by PCI SSC to indicate when the Vendor‘s full re-assessment is due.

A.7 Secure SLC Assessor Company

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

Appendix B Secure SLC Change Impact Template

This Change Impact Template is required for Administrative Change and Designated Change submissions for Secure SLC Qualified Vendor Listings. Always refer to the Program Guide for information on any Secure SLC Qualified Vendor Listing changes.

The Vendor must complete each section of this document and all other required documents based on the type of change. The Vendor is required to submit a completed report using this Change Impact Template along with supporting documentation to PCI SSC for review.

Part 1. Secure SLC Qualified Vendor Listing Details, Contact Information and Change Type

Vendor Listing Details			
Vendor Name		Qualified Listing Reference #	
Type of Change (Check one)	□ Administrative *(Complete Part 2)*	□ Designated *(Complete Part 3)*	
Submission Date			
Vendor Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	

Part 2. Details for Administrative Change (if indicated at Part 1)

Administrative Change Revision	
Current Vendor Company Name	
Revised Vendor Company Name (if applicable)	
Additional details, as applicable	

Part 3. Details for Designated Change (if indicated at Part 1)

Designated Change Revision		
Identify the type of designated changes applicable to this submission and complete the appropriate sections of this Secure SLC Qualified Vendor Change Impact Template (check all that apply). Refer to the Program Guide for details about each type of designated change.		
Add/Remove Category (Complete Part 3a)	□ Add	□ Remove
Description of changes to the Vendor Listing		
Description of how Designated Change impacts the Vendors Secure SLC functionality		
Additional details, as applicable		