Security Standards Council®

Payment Card Industry (PCI)

Software-based PIN Entry on COTS (SPoC)™

Program Guide

Version 1.3

May 2021

Document Changes

Date	Version	Description
April 2018	1.0	Initial Release of the PCI Software-based PIN Entry on COTS (SPoC) Program Guide
May 2019	1.1	Updated to support the use of PCI PTS-approved and non-PTS approved magnetic stripe readers (MSRs) in SPoC Solutions in accordance with the SPoC Magnetic Stripe Readers Annex (SPoC MSR Annex)
June 2020	1.2	Introduced the optional use of SPoC APIs (Application Programming Interfaces) provided by the SPoC Solution Provider to allow third-party developers to interface with the SPoC Solution Replaced Appendix D, "Documentation Required for SPoC Evaluation" with "SPoC Solution Provider-provided Libraries or APIs" Integrated various SPoC Technical FAQs v1.4 Dec 2019 (Q15, Q26, Q27) Removed Designated Changes, incorporated into the Delta Change process Introduced SPoC Solution Expired List for expired SPoC Solutions Added clarification around vendor-supported COTS Operating Systems and COTS System Baseline, consistent with the SPoC Standard Clarified that adding a new major version of a COTS device Operating System (i.e., v9.x, v10.x, etc.) may be considered Delta or High impact change per SPoC Lab's discretion Clarified various points and cleaned up typos and formatting issues throughout
May 2021	1.3	Updated to permit the use of unsupported operating systems (OS) in SPoC Solutions in accordance with the *SPoC Unsupported Operating System Annex* Clarified AOC requirements include PIN assessments for any key-injection facilities (KIFs) used in the SPoC Solution Clarified various points, cleaned up minor typos and formatting issues throughout

Table of Contents

1 Introduction1

1.1 SPoC Solution Overview 1
1.2 Related Publications 5
1.3 Updates to Documents and Security Requirements 6

2 Roles and Responsibilities 7

2.1 SPoC Vendors 7
2.1.1 Solution Providers 7
2.1.2 PIN CVM Application Vendors 7
2.1.3 Monitoring/Attestation System Vendors 8
2.1.4 Back-end Monitoring Environment Providers 8
2.1.5 SCRP Device Vendors 9
2.1.6 Magstripe Reader (MSR) Device Vendors 9
2.1.7 Third-Party Service Providers 10
2.2 Entities Involved in SPoC Evaluations 10
2.2.1 PCI-recognized SPoC Laboratories 10
2.2.2 PTS Labs (PCI-recognized Laboratories) 11
2.2.3 Participating Payment Brands 11
2.2.4 PCI Security Standards Council (PCI SSC) 12

3 Preparation for the Evaluation 13

3.1 Considerations for Elements Used in SPoC Solutions 13
3.2 Prior to the Evaluation 15
3.3 Required Documentation 16
3.4 Evaluation and Review Time Considerations 16
3.5 Technical Support throughout Testing 17
3.6 Vendor Release Agreement (VRA) 17
3.7 The Portal 18
3.8 SPoC Program Acceptance Fees 18

4 Evaluation and Reporting Processes 19

4.1 Required Solution Provider Materials 20
4.2 Supporting Multiple Platforms and Versions 21
4.3 Integrating SPoC Elements 22

5 Maintaining a Validated Solution Listing 25

5.1 Annual Checkpoints 25
5.2 Changes to SPoC Solution Listings 27
5.2.1 Administrative Changes for SPoC Solution Listings 28
5.2.2 Delta Changes 29
5.2.3 High impact Changes 30
5.3 Change Documentation 31
5.4 Acceptance and Change Fees 32
5.5 Renewing Expiring Listings 32
5.6 Validation Maintenance Fees 33
5.7 Notification Following a Security Breach, Compromise, or Known or Suspected Vulnerability . 33

6 Reporting Considerations 34

6.1 Evaluation Report Acceptance, Issuance of Approval Overview 34
6.2 Delivery of the Evaluation Report and Related Materials 35
6.2.1 Resubmissions... 35
6.3 Quality Management Programs 36
6.3.1 Evaluation Report Submission Review... 36

Appendix A SPoC Program Acceptance... 37

Appendix B Elements for the List of Validated SPoC Solutions 38

Appendix C Change Impact Template for SPoC Solutions.. 40

Appendix D SPoC Solution Provider-offered Libraries or APIs 47

Appendix E Software Versioning Methodology 49

Appendix F Terminology.. 51

1 Introduction

This Program Guide provides an overview of the PCI SSC Software-based PIN Entry on Commercial off-the-shelf (COTS) Standard (SPoC)™ program operated and managed by PCI Security Standards Council, LLC (PCI SSC). Use this guide with the documents referenced in Section 1.2, *Related Publications*. This document is primarily for Solution Providers who develop and PCI-recognized SPoC Laboratories (SPoC Labs) who validate SPoC Solutions. Capitalized terms used but not otherwise defined within this document have the meanings defined in or pursuant to *Appendix F* of this *Program Guide*.

This Program Guide describes the following:

- *Introduction* (Section 1)
- *Roles and Responsibilities* (Section 2)
- *Preparation for the Evaluation* (Section 3)
- *Evaluation and Reporting Processes* (Section 4)
- *Maintaining a Validated Solution Listing* (Section 5)
- *Reporting Considerations* (Section 6)

1.1 SPoC Solution Overview

A SPoC Solution (or Solution) comprises the following elements, each of which must be evaluated and validated for use in the Solution. Furthermore, the SPoC Solution itself must be evaluated and validated by a SPoC Lab before being submitted to PCI SSC for acceptance and Listing.

- **Secure Card Reader-PIN (SCRP) device:** A physical card reader that has been Evaluated by a PCI-recognized PIN transaction security (PTS) laboratory (PTS Lab), is listed on the PCI PTS Approved Device List on the Website with an SCRP Approval Class and can optionally support contact magnetic stripe reading functionality. For additional details, refer to the *SPoC Magnetic Stripe Readers Annex* (*SPoC* MSR *Annex)*.
- **Magnetic Stripe Reader (MSR):** Additional requirements apply to MSRs optionally used in SPoC Solutions. For details, refer to the *SPoC Magnetic Stripe Readers Annex* (*SPoC* MSR *Annex)*.

  ***Note:** PTS Technical FAQs on the Website may also apply to the MSR evaluation.*

- **PIN Cardholder Verification Method (CVM) Application (PIN CVM Application):** The PIN Cardholder Verification Application that has been Evaluated by a PCI-recognized SPoC Lab per the *SPoC Security Requirements* and *SPoC Testing Requirements* (*SPoC Standard*) as part of their SPoC Solution Evaluation. PIN CVM Applications are listed only as part of the SPoC Solutions in which they have been validated for use under the SPoC Program. PIN CVM Applications are not listed separately on the Website.
    - **SPoC Application Programming Interface (SPoC API):** An optional software component developed and provided by the Solution Provider to allow third-party developers to interface with the SPoC Solution. SPoC APIs must be Evaluated by a SPoC Lab as part of the Evaluation for each SPoC Solution with which a SPoC API is provided. SPoC APIs are listed only as part of the SPoC Solution in which they have been validated for use under the SPoC Program and are not listed separately on the Website.

***Note:** The PIN CVM Application (and/or optional API) must be validated along with its supporting Monitoring/Attestation System as part of each Solution in which it is used.*

- **Monitoring/Attestation System:** Evaluated by a SPoC Lab per the *SPoC Standard* as part of their SPoC Solution Evaluation. Monitoring/Attestation Systems are listed only as part of the SPoC Solutions in which they have been validated for use under the SPoC Program and are not listed on the Website.
- **Back-end Monitoring Environment:** The environment in which the Monitoring/Attestation System resides and operates must be assessed by a SPoC Lab for compliance with *SPoC Security Requirements*, Appendix A, "Monitoring Environment Basic Protections." Back-end Monitoring Environments are not listed on the Website.

Note: *If the Primary Account Number (PAN) or Sensitive Authentication Data (SAD) is stored, processed or transmitted in the Back-end Monitoring Environment, that environment is considered a Cardholder Data Environment (CDE) and must be assessed and validated by a Qualified Security Assessor (QSA) Company to the* PCI DSS*, including Appendix A3, "Designated Entities Supplemental Validation (DESV)."*

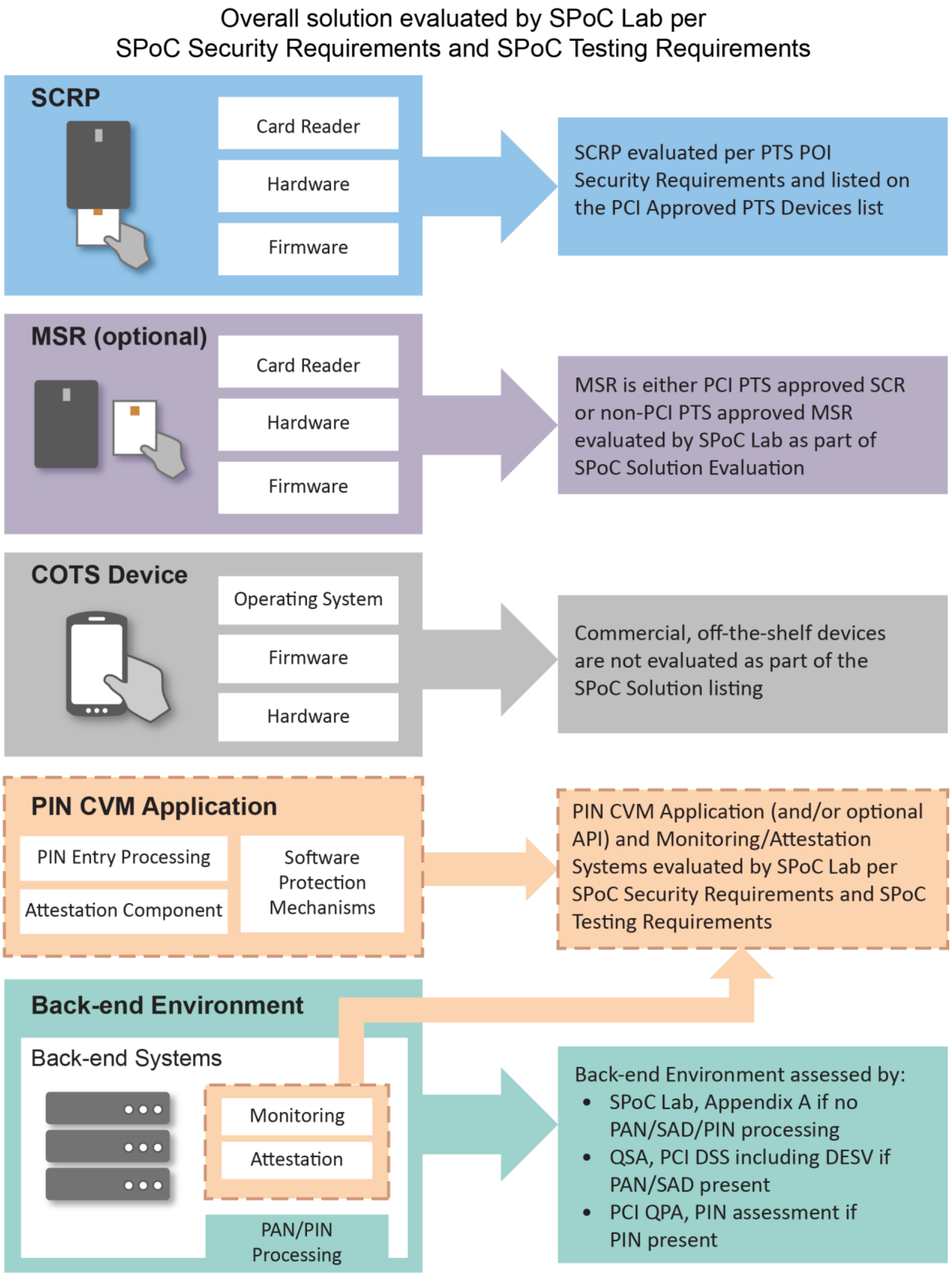
Note: *If PIN processing is performed in the Back-end Monitoring Environment, a full PIN audit is required in accordance with the PCI PIN Security Requirements.*

- **Back-end Processing Environment:** The environment where cardholder data and/or PIN data is decrypted and securely processed and, per the note above, must be validated for the following, where applicable:
    - – PCI DSS validation (AOC), issued within the past 12 months of the SPoC Evaluation Report submissions, by a QSA

- PCI PIN validation (AOC), issued within the past 12 months of the SPoC Evaluation Report submission by a PCI Qualified PIN Assessor (QPA), qualified by PCI SSC and listed on the Website as a QPA
- PCI PIN validation AOC(s) for any key-injection facility(s) (KIF) involved in injecting keys for the SCRP, issued within the past 12 months of the SPoC Evaluation Report submission, by a PCI Qualified PIN Assessor (QPA), qualified by PCI SSC and listed on the Website as a QPA

Figure 1 illustrates the elements of the SPoC Solution and the SPoC Program stakeholder that validates each element. For more detail, see the *SPoC Security Requirements,* “Overview” and “Software-based PIN Entry on COTS Devices” sections.

Figure 1: SPoC Solution Elements



Overall solution evaluated by SPoC Lab per
SPoC Security Requirements and SPoC Testing Requirements

SCRP evaluated per PTS POI Security Requirements and listed on the PCI Approved PTS Devices list

MSR is either PCI PTS approved SCR or non-PCI PTS approved MSR evaluated by SPoC Lab as part of SPoC Solution Evaluation

Commercial, off-the-shelf devices are not evaluated as part of the SPoC Solution listing

PIN CVM Application (and/or optional API) and Monitoring/Attestation Systems evaluated by SPoC Lab per SPoC Security Requirements and SPoC Testing Requirements

Back-end Environment assessed by:

- SPoC Lab, Appendix A if no PAN/SAD/PIN processing
- QSA, PCI DSS including DESV if PAN/SAD present
- PCI QPA, PIN assessment if PIN present

1.2 Related Publications

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

Document Name	Description
Payment Card Industry (PCI) Software-based PIN Entry on COTS Security Requirements ("SPoC Security Requirements")	The *SPoC Security Requirements* defines the specific technical security requirements for the Solution, including the PIN CVM Application, the supporting Monitoring/Attestation System and Back-end Monitoring Environment.
Payment Card Industry (PCI) Software-based PIN Entry on COTS Test Requirements ("SPoC Test Requirements")	The *SPoC Test Requirements* lists and defines the specific testing and Evaluation procedures required to evaluate the solution against the *SPoC Security Requirements*.
Payment Card Industry (PCI) Software-based PIN Entry on COTS (SPoC)™ Magnetic Stripe Readers Annex Security and Test Requirements ("SPoC MSR Annex")	The SPoC MSR Annex is a supplementary document to the *SPoC Security Requirements* and *SPoC Test Requirements* applicable to MSRs in listed SPoC Solutions.
Payment Card Industry (PCI) Software-based PIN Entry on COTS (SPoC)™ SPoC Unsupported OS Annex ("SPoC Unsupported OS Annex")	The SPoC Unsupported OS Annex is a supplementary document to the *SPoC Security Requirements* and *SPoC Test Requirements* applicable to unsupported operating systems used in listed SPoC Solutions.
SPoC Solution Attestation of Validation ("AOV")	The *AOV* is a form for SPoC Labs to use to attest to the results of a SPoC Solution Evaluation.
SPoC Solution Evaluation Report Template	The *SPoC Solution Evaluation Report Template* is the mandatory form that SPoC Labs must use to document the results of a SPoC Solution Evaluation.
Vendor Release Agreement ("VRA")	The *VRA* establishes the terms and conditions under which PCI SSC accepts and lists validated Solutions.

In addition to the documents listed in the table, see the current versions of the following documents, each of which is available on the Website:

- *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*
- *Payment Card Industry (PCI) Data Security Standard and Payment Application Data Security Standard Glossary of Terms, Abbreviations, and Acronyms (Glossary)*
- *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements ("PCI PTS POI Security Requirements")*
- *Payment Card Industry (PCI) PIN Security Requirements and Testing Procedures*

1.3 Updates to Documents and Security Requirements

This Program Guide may be modified to reflect updates to the SPoC Program. Additionally, PCI SSC provides interim updates to the PCI community through a variety of means, including required Assessor or Lab training, e-mail bulletins and newsletters, frequently asked questions (FAQs), and other communication methods.

Technical FAQs are updated on a regular basis to clarify the SPoC Program requirements and may also address new security threats. As such, technical FAQs supersede any specifically conflicting provisions of the Program Guide and are generally effective immediately upon publication. PCI SSC reserves the right to change, amend, or withdraw security requirements, training, and/or other requirements at any time.

2 Roles and Responsibilities

This section provides an overview of the roles and responsibilities of the various SPoC Program stakeholder groups.

2.1 SPoC Vendors

A Vendor or Solution Provider seeking Acceptance of its candidate SPoC Solution, PIN CVM Application, Monitoring/Attestation System or Back-end Monitoring Environment as part of the SPoC Program, must provide access to the applicable SPoC Solution or SPoC Elements and supporting documentation to its SPoC Lab for validation. The Vendor or Solution Provider must also authorize its SPoC Lab to submit resulting reports and related information to PCI SSC.

***Note:** SPoC Vendors/Solution Providers are responsible for assuring compliance with all applicable laws, statutes, regulations and rules (including without limitation, privacy laws) that apply to their activities as SPoC Vendors/Solution Providers and any related services or products.*

2.1.1 Solution Providers

Solution Providers (for example, processors, acquirers or payment gateways) have overall responsibility for the design and implementation of specific Solutions. They must ensure that their Solutions satisfy all applicable SPoC Security Requirements, managing Solutions for their customers and/or managing corresponding responsibilities.

2.1.2 PIN CVM Application Vendors

Software application vendors who develop PIN CVM Applications must submit those applications for Evaluation for secure operation. Vendors must provide the SPoC Lab with access to all corresponding unobfuscated source code and documentation that describe the secure installation and administration of such applications, including documentation associated with SCRPs that work with the PIN CVM Application.

The Solution Provider submits a PIN CVM Application and its supporting Monitoring/Attestation System for Evaluation to an independent SPoC Lab. Per the *SPoC Standard*, PIN CVM Application Vendors must provide documentation describing the secure operation and administration of such applications.

2.1.3 Monitoring/Attestation System Vendors

Monitoring/Attestation System vendors develop software applications that provide software-based tamper detection and response function (i.e., Monitoring/Attestation Systems) for a PIN CVM Application that is evaluated for use in a Solution. Monitoring/Attestation System vendors must submit their Monitoring/Attestation System for Evaluation and Validation per the *SPoC Standard* with each PIN CVM Application that it supports.

The Solution Provider submits a Monitoring/Attestation System for Evaluation to an independent SPoC Lab. Per the *SPoC Standard*, Monitoring/Attestation System vendors must provide documentation describing the secure operation and administration of such applications.

2.1.4 Back-end Monitoring Environment Providers

A Back-end Monitoring Environment provider must strictly maintain secure facilities to host Monitoring/Attestation Systems. To be used as part of a valid Solution, Back-end Monitoring Environments must have been evaluated within the preceding 12 months and validated by a SPoC Lab in accordance with the *SPoC Standard*.

- When a Monitoring/Attestation System resides in a Back-end Monitoring Environment provider's CDE, each Monitoring/Attestation System must also be validated by a QSA Company according to the *PCI DSS* including Appendix A3, "Designated Entities Supplemental Validation (DESV)."
- If PAN or SAD *is not present* in the Monitoring/Attestation System's environment and it *is not part* of the Back-end Monitoring Environment provider's existing CDE, a SPoC Lab must validate that the environment complies with the logical and physical security requirements defined in the *SPoC Standard,* Appendix A, "Monitoring Environment Basic Protections."

Note: *If the Solution Provider cannot meet DESV requirements at the point of an initial SPoC Solution validation, the Solution Provider must provide the SPoC Lab an action plan demonstrating that work is in progress for requirements to be met at the first annual checkpoint. The action plan will be reviewed by the SPoC Lab for sufficiency and submitted to PCI SSC as part of the Solution Evaluation process. Failure to meet DESV requirements by the first annual checkpoint may result in revocation of the SPoC Solution.*

Note: *If PIN processing is performed in the Back-end Monitoring Environment, a full PIN audit in accordance with the PCI PIN Security Requirements and Testing Procedures performed by a PCI QPA is also required and evidence submitted to the SPoC Lab as part of the Evaluation.*

2.1.5 SCRP Device Vendors

SCRP device vendors submit a SCRP devices to a PTS Lab for Evaluation. Per *PCI PTS POI Modular Security Requirements* (version 5.1 or later), SCRP device vendors must develop a supplemental document describing the secure operation and administration of such devices. For more detail, see *PCI PIN Transaction Security Device Testing and Approval Program Guide*.

***Note*: *Except as described in the* SPoC MSR Annex, *only validated SCRP devices that are listed on the PCI PTS Approved Device List are permitted for use in validated SPoC Solutions. For details about the use of MSRs, see the* SPoC MSR Annex*.*

2.1.6 Magstripe Reader (MSR) Device Vendors

To protect the Account Data read from magnetic stripe cards and deliver encrypted output to the payment processing systems, the MSR must conform with either:

- *PCI PTS POI Modular Security Requirements* with an SCR Approval Class

  ***Note:** The magnetic stripe reader must be listed as an approved PCI PTS device on the PCI PTS Approved Device list.*

  Or

- The security requirements identified in the *SPoC MSR Annex*. During the SPoC Solution Evaluation process (see sections 3, 4 and 6) a SPoC Lab must validate the MSR against specific requirements in section 4 of the *SPoC MSR Annex*.

  When an MSR is used in a SPoC Solution, only the device(s) included in the Solution Listing are validated/permitted for use in that Solution.

2.1.7 Third-Party Service Providers

Third-party service providers (such as KIFs) are considered Third-Party Service Providers with respect to the SPoC Element or SPoC Solution for which they provide services, and their services are evaluated/assessed as part of each SPoC Element and/or SPoC Solution. A Third-Party Service Provider must have its third-party services reviewed during each SPoC Solution Evaluation in which its service is used. Note that Third-Party Service Provider services that load key materials must comply with all applicable PCI PIN Security Requirements. Third-Party Service Providers are not eligible for Listing with regard to the SPoC Program.

2.2 Entities Involved in SPoC Evaluations

2.2.1 PCI-recognized SPoC Laboratories

PCI-recognized SPoC Laboratories (SPoC Labs) are qualified by PCI SSC to perform Evaluations of Solutions for Listing on the List of Validated SPoC Solutions. SPoC Labs are also qualified by PCI SSC to separately evaluate PIN CVM Applications and Monitoring/Attestation Systems to be used in Solutions as well as Back-end Monitoring Environment assessments (see the *SPoC Standard*, Appendix A “Monitoring Environment Basic Protections”). Listing of a SPoC Solution on the List of Validated SPoC Solutions signifies that the applicable SPoC Lab has determined that the Solution complies with all required criteria of the *SPoC Standard* and *Program Guide*. For the purposes of the SPoC Program, SPoC Labs are responsible for:

- Evaluating PIN CVM Applications, Monitoring/Attestation Systems, Back-end Monitoring Environments and overall SPoC Solutions in accordance with the *SPoC Standard*
- Evaluating conformance of non-PTS approved MSRs to the *SPoC MSR Annex*.
- Providing evidence to validate how the Solution meets the *SPoC Standard*
- Documenting each such Evaluation in an Evaluation Report using the applicable reporting template(s)
- Providing sufficient evidence within the Evaluation Report to demonstrate that the Solution complies with the *SPoC Standard*
- Where applicable, submitting the applicable Evaluation Report and/or any change submission documentation to PCI SSC, along with the applicable *SPoC Solution Attestation of Validation (AOV)* signed by both the SPoC Lab and Solution Provider
- Maintaining an internal quality assurance process for the SPoC Solution Evaluation efforts.

A PCI-recognized PTS Laboratory interested in becoming a SPoC Lab should contact PCI SSC for additional information.

2.2.2 PTS Labs (PCI-recognized Laboratories)

PTS Labs are responsible for the Evaluation of POI devices against PCI SSC's *PIN Transaction Security (PTS) Standards* and requirements (PTS requirements). Evaluation reports on devices validated as compliant with the PTS requirements are submitted by the PTS Lab to PCI SSC for approval; and if approved, the device is listed on the PCI PTS Approved Device List on the Website.

PTS Labs are authorized by PCI SSC to perform Evaluations of SCRP devices, PCI approved MSRs and magnetic stripe readers not currently classified as SCR; only PTS Labs are authorized by PCI SSC to Evaluate such devices used in SPoC Solutions.

Note: *SCRP device Evaluation by a PTS Lab is a separate process from the validation of a SPoC Solution; the SPoC Solution Evaluation validates whether a given Solution (which may include multiple SCRP devices) complies with the* SPoC Standard*.*

In addition to the above and for the purposes of the SPoC Program, PTS Labs are responsible for:

- Documenting each SCRP device or magnetic stripe reader Evaluation in a report
- Providing adequate documentation within the applicable report to demonstrate compliance with the *PCI PTS POI Modular Security Requirements* (or *SPoC MSR Annex)*.
- Where applicable, submitting applicable change submissions to PCI SSC, along with the applicable documentation signed by both the PTS Lab and SCRP (or MSR, as applicable) device Vendor
- Maintaining an internal quality assurance process for their Evaluation efforts

Note: *A PTS Lab is not authorized by PCI SSC to perform SPoC Solution Evaluations unless it is also qualified by PCI SSC as a SPoC Lab.*

2.2.3 Participating Payment Brands

The Participating Payment Brands independently develop and enforce the various aspects of their respective programs related to compliance with PCI SSC Standards, including, but not limited to:

- Defining security and program requirements for merchant and service provider levels
- Managing compliance enforcement programs (requirements, mandates, or compliance dates)
- Establishing penalties and fees

- Establishing requirements and who must validate
- Responding to cardholder data compromises

2.2.4 PCI Security Standards Council (PCI SSC)

PCI SSC is the standards body that maintains the PCI SSC Standards. In relation to the *SPoC Standard*, PCI SSC:

- Hosts the List of Validated SPoC Solutions on the Website
- Maintains a centralized repository for all Evaluation reports for Solutions listed on the Website
- Qualifies SPoC Labs to evaluate and validate SPoC Solutions and SPoC Elements for compliance with the *SPoC Standard*
- Maintains and updates the *SPoC Standard* and related documentation including FAQs; and
- Reviews all Solution Evaluation Reports and related change submissions submitted to PCI SSC for quality assurance and compliance with baseline quality standards.

PCI SSC does not evaluate, assess, or validate SPoC Elements or SPoC Solutions for SPoC compliance—these tasks are performed by the SPoC Labs. Listing of a Solution on the List of Validated SPoC Solutions signifies the following:

- The SPoC Lab has determined that the Solution complies with the *SPoC Standard*
- The SPoC Lab has submitted a corresponding Solution Evaluation Report to PCI SSC
- The Solution Evaluation Report satisfied all PCI SSC requirements as of the time of the review.

***Note:** PCI SSC does not assess or validate SPoC Solutions for compliance with the SPoC Standard. PCI SSC acceptance and subsequent listing of a SPoC Solution on the List of Validated SPoC Solutions signifies that the applicable SPoC Lab has determined that the Solution complies with all required criteria of the SPoC Standard and Program Guide, that the SPoC Lab has submitted a corresponding Evaluation Report to PCI SSC, and that the Evaluation Report, as submitted to PCI SSC, has satisfied all applicable quality assurance review requirements as of the time of PCI SSC's review. The SPoC Lab is ultimately accountable for the completeness and accuracy of the materials provided to PCI SSC.*

3 Preparation for the Evaluation

The *SPoC Standard* is a cross-functional PCI SSC standard that includes specific requirements that have been validated through the PCI SSC PTS Program and, where applicable, the PCI DSS Assessment/QSA Program and/or the PCI PIN Program. The *SPoC Standard* also contains requirements for SPoC Solutions and SPoC Elements (SCRPs, optional MSRs, PIN CVM Applications, Monitoring/Attestation Systems and Back-end Monitoring Environments) that are used in the SPoC Solution.

***Note**: SPoC Solution Providers, SPoC Labs and Assessors are expected to be acutely familiar with each module within the* SPoC Standard *before commencing an Evaluation.*

3.1 Considerations for Elements Used in SPoC Solutions

Table 1 describes the requirements and eligibility for various elements used in SPoC Solutions, including references to the relevant documents and document sections.

Table 1: SPoC Solution Elements

Element	Program Guidance
SCRP	Secure Card Reader – PIN (SCRP) is a PTS approval class that supports PIN entry on COTS devices in accordance with the *PCI PTS POI Modular Security Requirements* (version 5.1 or higher). PTS device approval helps to ensure that the device has been evaluated and meets industry recognized requirements for payment acceptance devices. SCRPs are listed on the PCI PTS Approved Device List on the Website. The Solution must permit the use of only SCRPs listed on the Website. • See the *SPoC Standard Module 6*, "Secure Card Reader (SCRP)" • See the *PCI PTS POI Modular Security Requirements* (version 5.1 or later) and supporting documentation in the Document Library on the Website. The secure-card reader vendor is responsible for obtaining and maintaining PTS Program device approval. For devices that require approval, such approval is a prerequisite for the devices that are part of a SPoC Solution Evaluation. As part of a Solution Evaluation, SPoC Labs request evidence that PTS Program device approvals are current. SPoC Labs shall obtain all AOCs as evidence for any key-injection facility(s) (KIF) involved in injecting keys for the SCRP, verify it is current (i.e., issued within the past 12 months of the SPoC Evaluation Report submission), and submit the AOC(s) via the Portal with the SPoC Evaluation Report. Device vendors who seek device approval under the PTS Program should consult the Website for further information. PTS Program approval does not replace or supersede any Participating Payment Brand-specific device-approval processes.
COTS platform and Operating System	While evaluation of the COTS device itself (e.g., device model, platform and Operating System (OS)) is out of scope for the purposes of SPoC Evaluation, only COTS OSs supported by the OS vendor at the time of the Evaluation, or SPoC Solutions evaluated and validated to security requirements in the *SPoC Unsupported OS Annex* will be accepted for approval and listing by PCI SSC. Multiple major versions of a vendor-supported OS (e.g., 8.x, 9.x, etc.) are permitted for inclusion in a single SPoC Evaluation Report. The SPoC Lab will test and report on each major OS version, for each test requirement, and all major versions of the OS submitted and validated will be listed as part of the SPoC Solution in which they are included. Support for different COTS *platforms* (e.g., Android, iOS, etc.) are considered separate SPoC Solutions, and therefore require separate Evaluation reports, validation and listings on the Website.

Element	Program Guidance
MSR	Magnetic Stripe Reader (MSR) is an optional element in a SPoC Solution. As specified in the *SPoC MSR Annex*, MSRs are not permitted to obtain a PIN when used in a SPoC Solution. MSRs must encrypt account data in accordance with the *SPoC Standard* (including *SPoC MSR Annex* as applicable) to prevent exposure within the PIN CVM Application and to ensure that encrypted data is transmitted securely to the Back-end Processing Environment. MSRs are classified as follows: • MSRs that are listed by PCI SSC as approved devices (with the Approval Class SCR) in the PCI PTS POI Program and fully meet the Evaluation Module 4 (SRED) of the *PCI PTS POI Security Requirements* • MSRs that are not listed by the PCI PTS POI Program but meet the security requirements listed in the *SPoC MSR Annex*, Section 4, Non-PTS Listed MSR Security Requirements and Derived Test Requirements Both PTS-listed MSRs (evaluated by a PTS Lab) and non-PTS-approved MSRs (evaluated by a SPoC Lab) must be evaluated using the PCI PTS POI test procedures as identified in the *PCI PTS POI Derived Test Requirements.* Note that PTS Technical FAQs on the Website may also apply to the MSR evaluation. Details for both PTS-listed and non-PTS approved MSRs are included on the List of Validated SPoC Solutions under “Solution Details” in each Solution for which the MSRs are validated. See the *SPoC MSR Annex*.
PIN CVM Application	PIN CVM Applications must be validated by a SPoC Lab against: • *SPoC Standard*, including Module 2, “PIN Cardholder Verification Method (CVM) Application” • *SPoC Standard*, Appendix D, “Application Security Requirements” • *SPoC Test Requirements Module 2*, “PIN CVM Application Requirements” A PIN CVM Application (and its supporting Monitoring/Attestation System) may be used in multiple Solutions. However, the PIN CVM Application is considered a SPoC Element only of the specific Solution(s) for which it has been tested and validated in accordance with SPoC Program requirements. ***Note:*** If the PIN CVM Application and/or the supporting Monitoring/Attestation System requires any additional software to be installed on the SCRP device, that software must also be tested and validated as part of the Solution Evaluation.
Monitoring/ Attestation System (“Monitoring System”)	Monitoring/Attestation Systems must be validated by a SPoC Lab against: • *SPoC Standard*, including Module 3, “Back-end Systems – Monitoring/Attestation” • *SPoC Standard,* Module 4, “Solution Integration Requirements” • *SPoC Test Requirements*, Module 3, “Back-end System Monitoring/Attestation Requirements” A Monitoring/Attestation System (and the PIN CVM Application it supports) may be used in multiple Solutions. However, the Monitoring/Attestation System is considered a SPoC Element only of the specific Solution(s) for which it has been tested and validated in accordance with SPoC Program requirements.

Element	Program Guidance
Back-end Monitoring Environment	The Back-end Monitoring Environment must be validated against all applicable requirements in the *SPoC Standard*, including Module 5, “Back-end Systems – Processing,” and Security Requirements Appendix A, “Back-end Monitoring Environment Basic Protections.” • If PAN or SAD is present anywhere in the Back-end Monitoring Environment, then PCI DSS plus DESV compliance as validated by a QSA is required. In such cases, the Solution Provider’s PCI DSS Attestation of Compliance (AOC) would be provided to the SPoC Lab during the SPoC Solution Evaluation as evidence of a compliant Back-end Monitoring Environment. SPoC Labs shall obtain the AOC as evidence, verify it is current (i.e., issued within the past 12 months of the SPoC Evaluation Report submission), and submit the AOC via the Portal with the SPoC Evaluation Report. ***Note:*** *If the Solution Provider cannot meet DESV requirements at the point of an initial SPoC Solution validation, the Solution Provider must provide the SPoC Lab an action plan demonstrating that work is in progress for requirements to be met at the first annual checkpoint. The action plan will be reviewed for sufficiency.* • If PIN processing (e.g., decryption or translation) is performed in the Back-end Monitoring Environment, a full PIN audit in accordance with the PCI PIN Security Requirements and Testing Procedures performed by a PCI QPA is also required. SPoC Labs shall obtain the AOC as evidence, verify it is current (i.e., issued within the past 12 months of the SPoC Evaluation Report submission) and submit the AOC via the Portal with the SPoC Evaluation Report.
Back-end Processing Environment (if separated from the Back-end Monitoring Environment)	The Back-end Processing Environment, where cardholder data and/or PIN data is decrypted and securely processed, must be validated for the following, where applicable: • PCI DSS validation (AOC) by a QSA • PCI PIN validation (AOC) by a PCI QPA • Key-injection facility(s) (KIF) validation AOC(s) by a PCI QPA for any key-injection facility(s) (KIF) involved in injecting keys for the SCRP SPoC Labs shall obtain the AOC(s) as evidence, verify they are current (i.e., issued within the past 12 months of the SPoC Evaluation Report submission), and submit the AOC(s) via the Portal with the SPoC Evaluation Report according to *SPoC Test Requirements* E1 and E2.

3.2 Prior to the Evaluation

Note: *The Solution development and test process is defined in the* SPoC Standard*. This document(s) includes guidance for implementing requirements, testing and validating compliance with each requirement*.

Before starting a SPoC Solution Evaluation (Evaluation), all involved parties involved are encouraged to take the following preparatory actions:

- Review the *SPoC Standard,* technical FAQs and all related documentation on the Website.
- Determine the Solution’s readiness to comply with the *SPoC Standard*:
  - Perform a gap analysis between the candidate solution’s security functions and the *SPoC Standard*;
  - Correct any gaps; and
  - If desired, the SPoC Lab may perform a pre-Evaluation or gap analysis of a candidate SPoC Element or candidate SPoC Solution. If the SPoC Lab notes deficiencies that

would prevent a compliant result, the SPoC Lab may provide a list of issues to the Solution Provider to be addressed before the formal Evaluation process begins.

- SPoC Solution Providers are responsible for ensuring that the various elements used as parts of their Solutions are each compliant with all applicable SPoC Security Requirements; and that the appropriate agreements are in place with the providers and vendors of these elements to ensure proper information disclosures if required under the Vendor Release Agreement.
- While SPoC Security Requirement 2.2.2 requires that PIN CVM Applications must be developed only for operating systems (OS) that are supported by the OS vendor, PCI SSC has published an optional *SPoC Unsupported OS Annex* which outlines additional security controls to allow SPoC Solution providers to support COTS devices with unsupported operating systems. Otherwise, all new SPoC Solutions must operate only on supported platforms and the COTS System Baseline (see the *SPoC Standard*) must only include versions of a COTS OS that is supported by the OS vendor at the time of Evaluation.

Note: *The SPoC Unsupported OS Annex must be used if the SPoC Solution uses any unsupported operating systems.*

3.3 Required Documentation

When submitting a Solution for initial Evaluation and Listing, the Solution Provider must provide the SPoC Lab with the documentation described in the SPoC Standard including any applicable Annexes. The SPoC Lab should be prepared to submit documentation such as the Vendor Release Agreement, completed SPoC Solution Evaluation Report and applicable AOC(s) to PCI SSC as described throughout this Program Guide.

Note: *All completed Evaluation materials, such as manuals, install guides, and the Vendor Release Agreement, must be delivered to the SPoC Lab performing the Evaluation—not to PCI SSC.*

3.4 Evaluation and Review Time Considerations

The amount of time necessary for the SPoC Lab to complete its work can vary widely depending on factors such as:

- Candidate Solution or element initial level of compliance with the SPoC Standard and Program requirements—more corrections mean a longer review and validation
- Prompt payment of fees to PCI SSC—PCI SSC will not start the review process until the applicable fees are paid
- Quality of the SPoC Lab's Evaluation Report submitted to PCI SSC. For example:
  - Incomplete submissions or errors. For example, missing, incomplete or unsigned documents will delay the review and acceptance process

- Multiple review/correction iterations between the PCI SSC and the SPoC Lab will delay the review and acceptance process.

Any Evaluation completion dates that the SPoC Lab provides should be considered estimates. The SPoC Lab may base the completion date on the assumption that the candidate Solution or Element will meet all SPoC Program requirements quickly. If problems arise during the review or acceptance process, discussions between the SPoC Lab, the Solution Provider and PCI SSC may delay or prematurely end the Evaluation. For example, an Evaluation may end if the Solution Provider decides not to make the changes necessary to achieve compliance. Back-end Monitoring Environment Assessments (including PCI DSS Assessments or PCI PIN audits, as applicable) may require additional time—the Solution Provider should consider this when planning the Evaluation schedule.

Note: *For details about PCI SSC review times, see Section 6.1, Evaluation Report Acceptance, Issuance of Approval Overview.*

3.5 Technical Support throughout Testing

A Solution Provider technical representative should be available to assist with questions that may arise during the Evaluation. To expedite the review process, a technical representative should be on call to discuss issues and respond to questions from the SPoC Lab.

3.6 Vendor Release Agreement (VRA)

Before PCI SSC reviews any Solution (or candidate Solution) for Listing on the Website, the Solution Provider must provide a signed copy of the current Vendor Release Agreement (VRA) to the SPoC Lab. The current version of the VRA is available on the Website. In addition, at the beginning of each SPoC Solution Evaluation, the Solution Provider provides access to the Solution and other documents and materials.

Among other things, the VRA addresses the following topics:

- Confidentiality issues
- Solution Provider's agreement with the SPoC Program requirements, policies, and procedures
- Permission for the Solution Provider's SPoC Lab to release Evaluation Reports, AOVs, and related materials to PCI SSC for review
- Solution Provider's agreement to adopt and comply with industry standard vulnerability handling policies.

For PCI SSC to review an Evaluation Report, the SPoC Lab must provide PCI SSC with the Solution Provider-signed copy of the VRA.

While an executed copy of the then most current version of the VRA (available on the Website) is on file with PCI SSC for the respective Solution Provider, the SPoC Lab is not required to resubmit the same VRA with each subsequent Evaluation Report for the same Solution Provider.

3.7 The Portal

For any Solution to be listed on the Website, all documents relating to the validation of the corresponding candidate Solution are to be submitted by the applicable SPoC Lab, on behalf of the Solution Provider, to PCI SSC through PCI SSC's secure website (Portal). PCI SSC staff pre-screens submissions in the Portal to ensure that all required documentation has been included and the basic submission requirements have been satisfied. The Portal is also used by PCI SSC and SPoC Labs to track communications relating to a submission.

3.8 SPoC Program Acceptance Fees

For each Solution to be listed on the Website, the Solution Provider is also required to pay an Acceptance Fee to PCI SSC. For each new Solution submission, the corresponding Acceptance Fee will be invoiced and must be received by PCI SSC before the submission will be reviewed, Accepted and added to the List of Validated SPoC Solutions. Upon Acceptance, PCI SSC will sign and return a copy of the corresponding AOV to both the Solution Provider and the SPoC Lab.

Note: *All Evaluation-related fees are payable directly to the Lab (these fees are negotiated between the Lab and its customers). PCI SSC will bill the Solution Provider for all Acceptance Fees, and the Solution Provider will pay these fees directly to PCI SSC.*

There are no annual recurring PCI SSC fees associated with the Acceptance of a SPoC Solution or SPoC Element. There are, however, PCI SSC fees associated with Solution Provider delays in annual revalidation of a Validated SPoC Solution. See the Fee Schedule on the Website for more information.

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

4 Evaluation and Reporting Processes

The following provides an overview of the SPoC Solution Evaluation process.

1. The SPoC Solution Provider contracts with a SPoC Lab to perform an Evaluation of the candidate Solution and negotiates the cost and any associated confidentiality and non-disclosure agreements with the SPoC Lab.
2. The Solution Provider provides the SPoC Lab with access to all SPoC Elements to be used in the Solution to be evaluated, including the VRA, associated manuals and other required documentation and access to systems (including onsite access if required) as the SPoC Lab must perform appropriate testing and cannot rely solely on evidence submitted by the Solution Provider. For information about required documentation and materials, see Section 3.3, Required Documentation. The SPoC Lab may also require access to the Back-end Monitoring Environment for evaluation and/or to validate the Monitoring/Attestation System functionality.

   ***Note:** When the Monitoring/Attestation System resides in a cardholder data environment (CDE), the environment must adhere to* PCI DSS*, including DSS Appendix A3: Designated Entities Supplemental Validation (DESV).*

   *If PAN or SAD is **not** present in the Monitoring/Attestation System's environment (i.e., it is not part of a CDE), the environment must comply with the logical and physical security requirements defined in the* SPoC Standard*, Appendix A, "Back-end Monitoring Environment Basic Protections."*

3. The SPoC Lab performs the SPoC Solution Evaluation, including Evaluation of security functions and features. The Evaluation determines whether the candidate Solution and its associated elements comply with the *SPoC Standard*. The Solution and elements are validated in accordance with the *SPoC Test Requirements*.

   Note*: If any element of a SPoC Solution is evaluated by an entity other than the SPoC Lab performing the current Evaluation, the evaluating SPoC Lab should have access to all associated report(s) and supporting evidence. If those reports are not available for any reason, the evaluating SPoC Lab must determine the extent of additional work required to properly evaluate and attest to the Solution's compliance with the SPoC Standard.*

   If the evaluating SPoC Lab is unable to rely on the information – whether available or unavailable – and the SPoC Lab is unable to perform the additional work required to achieve such reliance, PCI SSC will be unable to accept the report.

   In all cases, PCI SSC may reject the report if (in the judgment of PCI SSC) the report does not contain adequate information to substantiate the conclusions of compliance with the SPoC Standard.

4. The SPoC Lab completes the Evaluation Report.

5. If the SPoC Lab determines that the Solution complies with the *SPoC Standard*, the SPoC Lab submits the corresponding Evaluation Report and AOV (for each Solution), the Solution Provider's signed VRA, Solution Provider's Back-end Environment AOC(s), if applicable, and any other requested documentation to PCI SSC via the Portal in accordance with applicable PCI SSC templates, guidance and instructions.
6. If required, the Solution Provider performs remedial activities to address security objectives or requirements that are not in place, or security controls for which there was insufficient evidence. The SPoC Lab then performs follow-up testing and provides PCI SSC with an updated Evaluation Report.
7. PCI SSC issues an invoice to the Solution Provider for the applicable Acceptance Fee. After the Solution Provider pays the invoice, PCI SSC reviews the Evaluation Report to confirm that it meets the SPoC Program requirements and if confirmed, PCI SSC notifies the SPoC Lab and Solution Provider that the Solution has successfully completed the process.
8. PCI SCC countersigns the AOV and sends a copy to the Solution Provider and the SPoC Lab.
9. PCI SSC adds the Solution to the List of Validated SPoC Solutions on the Website.

***Note**: To be listed on the List of Validated SPoC Solutions, a Solution must, at a minimum, contain one of each successfully validated SCRP, PIN CVM Application, and Monitoring/Attestation System and be implemented in a Back-end Monitoring Environment that meets all applicable requirements.*

4.1 Required Solution Provider Materials

The Solution Provider must provide sufficient evidence to enable a SPoC Lab to validate the Solution against the *SPoC Standard*. Such evidence may be in the form of formal documentation, such as policies and procedures, or informal documentation, such as design documents, data-flow diagrams, process descriptions, and results of internal analysis or testing (see Section 3.3, Required Documentation for additional details). However, any evidence must clearly and concisely show that the security controls implemented by the Solution Provider conform to the security objectives and requirements. This evidence must also show the ongoing effectiveness of those security controls.

Additionally, the Solution Provider must provide access to the following:

- All production-level, unobfuscated source code.
- All production-level, obfuscated code for all internally developed function, including bespoke or custom functionality developed by third parties.

Failure to provide adequate access to source code shall be considered a failure to meet applicable security objectives and requirements.

Note: *In cases where a Solution Provider or SPoC Solution/SPoC Element cannot meet a specific requirement as stated, the Solution Provider must clearly explain why the requirement cannot be met as stated. The Solution Provider must also provide evidence to clearly show how the corresponding security objective is still being met or exceeded, and that the alternative controls or methods that are employed provide equivalent or greater assurance to that provided by the methods described in the requirement. Solution Providers should work with their SPoC Lab to determine the evidence required to satisfy a specific security objective or associated requirement. The SPoC Lab is responsible for evaluation of the alternative controls or methods, and must include in the Evaluation Report a description of the testing they performed, justification of how the testing confirms the security objective has been met or exceeded and a statement confirming that the security objective has been met or exceeded.*

4.2 Supporting Multiple Platforms and Versions

Each new validation (or revalidation of an existing SPoC Solution) requires Evaluation against the then-current version of the *SPoC Standard*. Solutions for different major versions of the *SPoC Standard* (e.g., version 1.x, version 2.x) represent different SPoC Solutions, therefore, each update to a Solution to a new major version of the *SPoC Standard* requires a new, complete (full) Evaluation of the entire SPoC Solution.

Updating a SPoC Solution listing to a minor version of the *SPoC Standard* (for example, from version 1.0 to version 1.1) may be performed via Delta Evaluation if determined eligible by the SPoC Lab. The SPoC Lab must use their discretion to determine the level of testing that must be performed to gain sufficient assurance that the Solution complies with all applicable SPoC Security Requirements.

Support for different major versions of COTS device *operating systems* (e.g., 9.x, 10.x, etc.) are permitted in a single SPoC Solution Evaluation and listing on the Website. However, support for different COTS *platforms* (e.g., Android, iOS, etc.) are considered separate SPoC Solutions, and therefore require separate, full SPoC Evaluation Reports, validation and listings on the Website.

4.3 Integrating SPoC Elements

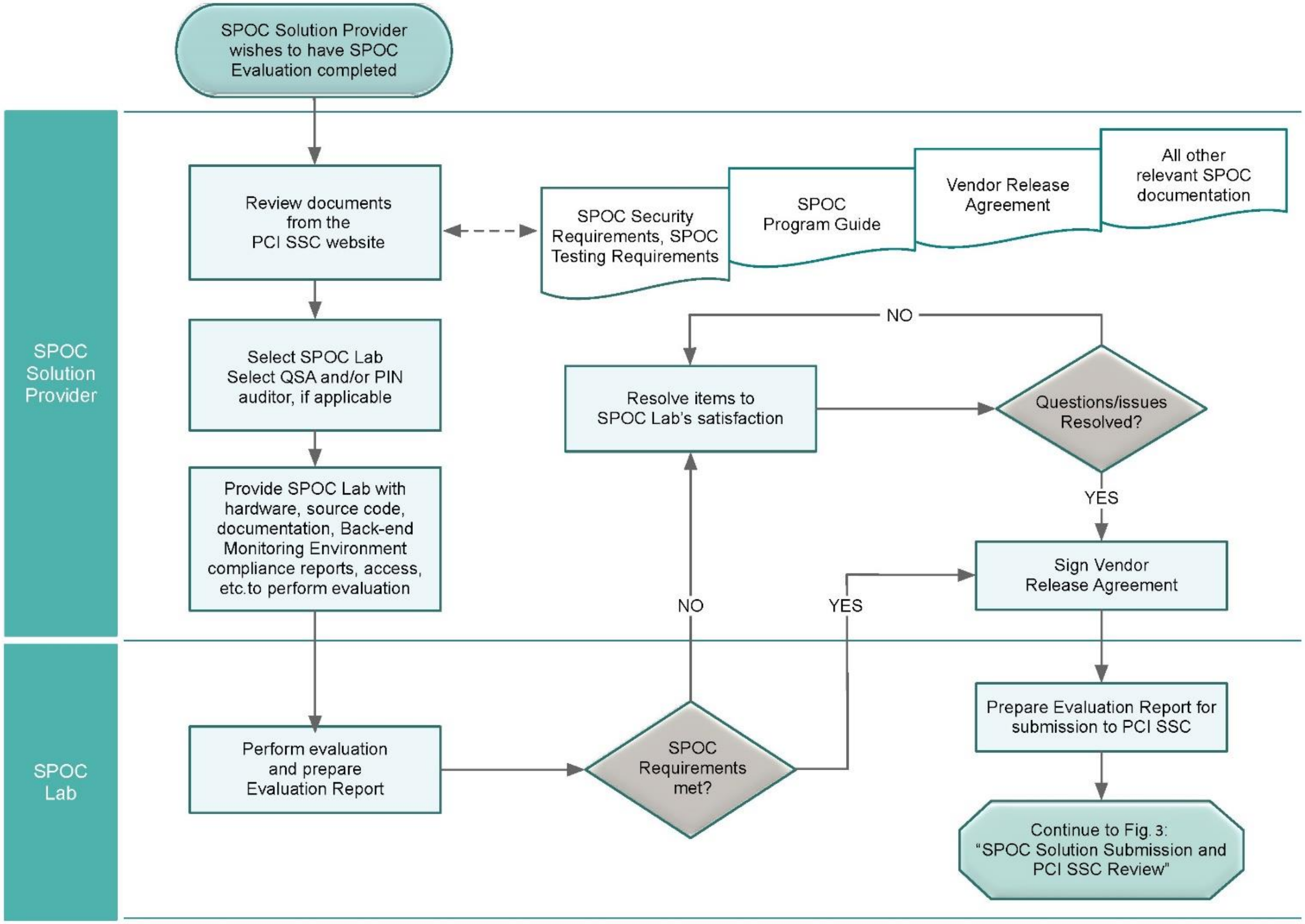
SPoC Solutions that leverage security services from elements defined within the SPoC architecture and which reside outside the formal technical boundary of the Solution (for example, at the COTS device or operating system level) will also require validation as part of the Evaluation. SPoC Solution Providers who use these services are responsible for obtaining and providing all evidence and materials necessary to support validation of these elements to the satisfaction of the SPoC Lab. Moreover, as part of the Evaluation, the SPoC Lab must evaluate the interaction between the Solution and the external security services.

In cases where the SPoC Solution Provider offers a SPoC API or software libraries to allow third parties to interface the Solution, Evaluation and validation by a SPoC Lab is required as part of each SPoC Solution in which such SPoC APIs are provided in order to validate that third-party usage of the SPoC API cannot affect the Solution's functionality or compliance with the *SPoC Standard*. See Appendix D for additional details.

Note: *SPoC Solution Providers are responsible for providing all evidence, materials and access necessary to support validation of these elements by the SPoC Lab.*

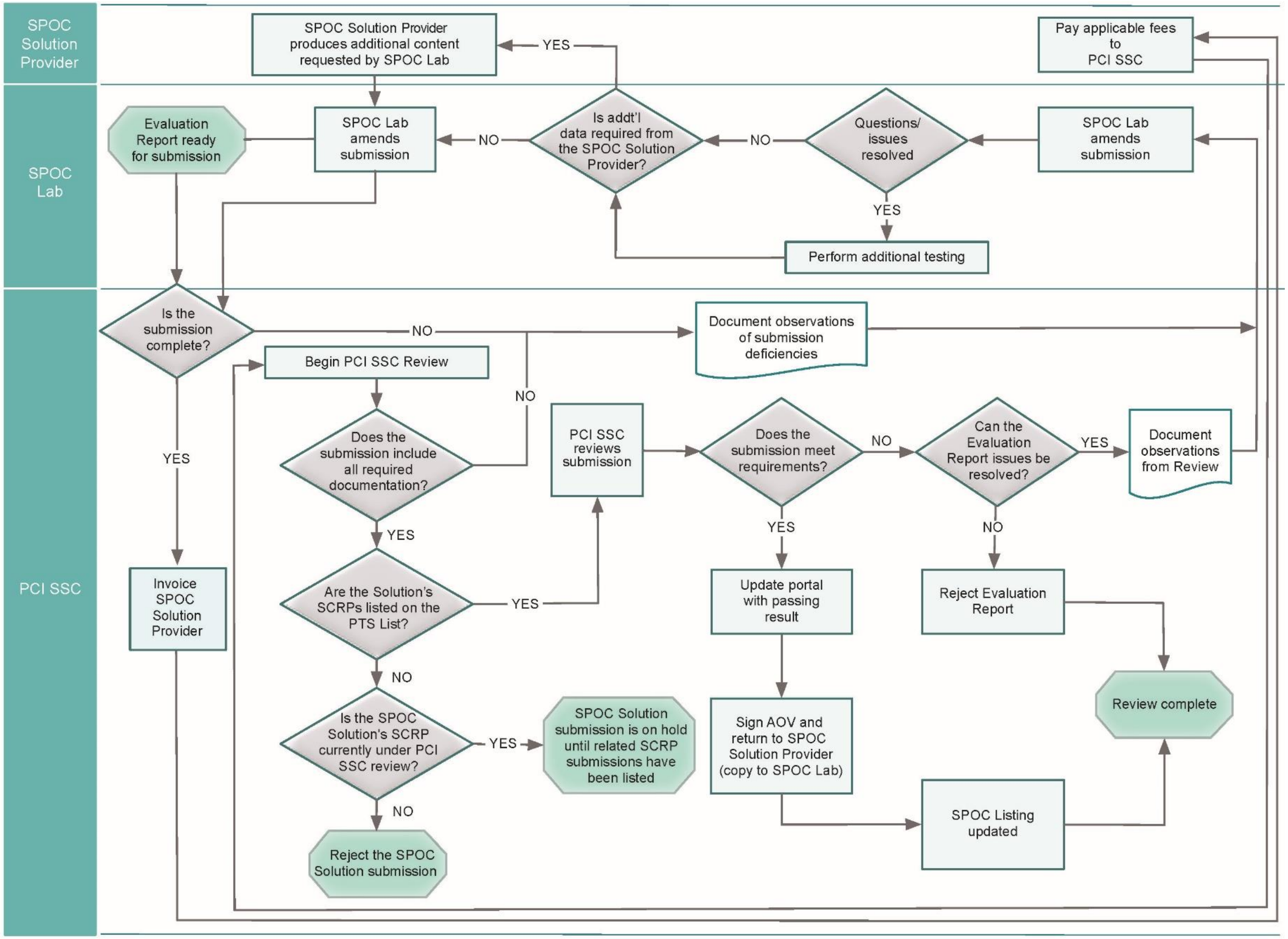
Figure 2 shows the SPoC Solution Evaluation and PCI SSC Listing process. Figure 3 shows the SPoC Solution submission and PCI SSC review process.

Figure 2: SPoC Solution Evaluation for PCI SSC Listing



SPOC Solution Provider wishes to have SPOC Evaluation completed
SPOC Solution Provider
SPOC Lab
Review documents from the PCI SSC website
SPOC Security Requirements, SPOC Testing Requirements
SPOC Program Guide
Vendor Release Agreement
All other relevant SPOC documentation
Select SPOC Lab Select QSA and/or PIN auditor, if applicable
NO
Resolve items to SPOC Lab's satisfaction
Questions/issues Resolved?
YES
Provide SPOC Lab with hardware, source code, documentation, Back-end Monitoring Environment compliance reports, access, etc.to perform evaluation
NO
YES
Sign Vendor Release Agreement
Prepare Evaluation Report for submission to PCI SSC
Perform evaluation and prepare Evaluation Report
SPOC Requirements met?
Continue to Fig. 3: "SPOC Solution Submission and PCI SSC Review"

Figure 3: SPoC Solution Submission and PCI SSC Review



SPOC Solution Provider
SPOC Lab
PCI SSC
SPOC Solution Provider produces additional content requested by SPOC Lab
YES
Pay applicable fees to PCI SSC
Evaluation Report ready for submission
SPOC Lab amends submission
NO
Is addt'l data required from the SPOC Solution Provider?
NO
Questions/ issues resolved
SPOC Lab amends submission
YES
Perform additional testing
Is the submission complete?
NO
Document observations of submission deficiencies
Begin PCI SSC Review
NO
Does the submission include all required documentation?
PCI SSC reviews submission
Does the submission meet requirements?
NO
Can the Evaluation Report issues be resolved?
YES
Document observations from Review
YES
YES
YES
NO
Invoice SPOC Solution Provider
Are the Solution's SCRPs listed on the PTS List?
YES
Update portal with passing result
Reject Evaluation Report
NO
Review complete
Is the SPOC Solution's SCRP currently under PCI SSC review?
YES
SPOC Solution submission is on hold until related SCRP submissions have been listed
Sign AOV and return to SPOC Solution Provider (copy to SPOC Lab)
NO
SPOC Listing updated
Reject the SPOC Solution submission

5 Maintaining a Validated Solution Listing

This section describes requirements for reevaluation of validated Solutions. Annual reevaluations are required on or before each one (1) year anniversary of the original date of Acceptance, in three (3) year cycles. Solutions require an annual *checkpoint*, on or before each annual checkpoint date in each three-year cycle, and a new full Evaluation on or before the Reevaluation Date (the expiry date).

Note**:** *Solutions require a full Evaluation every three years.*

5.1 Annual Checkpoints

Solution Providers are required to perform checkpoints at 12- and 24-month intervals from the date of Acceptance, including the submission of an updated *SPoC Solution AOV* to PCI SSC. Each annual checkpoint submission must be made by a SPoC Lab. SPoC Labs must review all changes that have occurred since the last full Evaluation or last annual checkpoint (whichever is more recent) and consider any applicable Delta Changes that have been validated during the previous 12-month period. The SPoC Lab must also perform live testing to ensure that the Solution remains compliant with all applicable SPoC Security Requirements. Live testing means full testing of active production-level COTS devices, PIN CVM Application, and its Monitoring/Attestation System.

PCI SSC typically provides a courtesy reminder via e-mail to the Solution Provider’s Primary Contact (listed on the AOV) within 90 calendar days of each checkpoint. However, it is the sole responsibility of the Solution Provider to comply with checkpoint requirements and maintain its Listings, regardless of courtesy reminders.

Note: *Solution Providers should submit annual checkpoint documentation and attestation to the SPoC Lab that performed the last full SPoC Solution Evaluation, as changing SPoC Labs requires a full SPoC Solution Evaluation.*

As part of the annual checkpoint process, the Solution Provider must confirm any changes that have been made to the Solution, and that:

- Changes have been applied in a way that is consistent with the *SPoC Standard*.
- The Solution continues to meet all applicable SPoC Security Requirements.

  Note: *In cases where the SPoC Solution Provider wants to allow COTS devices with unsupported OS, the SPoC Lab must perform additional testing to confirm security objectives outlined in the SPoC Unsupported OS Annex are met.*

- PCI SSC has been advised of any change that requires a change to the Listing on the Website, in accordance with this *Program Guide*.
- Changes to the documents described in the SPoC Standard are provided to the SPoC Lab for review annually (12-month and 24-month checkpoints).
- The operational quality of the Monitoring/Attestation System has been assessed according to *SPoC Test Requirements*, Appendix B.

The Solution Provider must consider the impact of external threats and whether updates to the Solution are necessary to address these threats. The SPoC Lab submits the updated AOV, redlined Evaluation Report, Solution Provider's Back-end Environment AOC(s), if applicable, and any applicable documentation to PCI SSC using the Portal.

An updated AOV and redlined Evaluation Report must be submitted to PCI SSC up to 60 calendar days ahead of the annual checkpoint date. PCI SSC has 30 calendar days to review and accept the submission. If PCI SSC does not receive the submission before the annual checkpoint date, the Listing will be subject to early administrative expiry, as follows:

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

- Fourteen (14) calendar days following the annual checkpoint date, the corresponding Listing will be updated to show the Listing's annual checkpoint date in **Orange** for a period of 90 calendar days past the annual checkpoint date.
- If the updated and complete AOV is received within this 90-day period, PCI SSC will update the corresponding Listing's annual checkpoint date with the new date and remove the **Orange** status.
- If the updated and complete AOV is not received within this 90-day period, the corresponding Listing's annual checkpoint date will be updated to show the date in **Red** for a period of no longer than 90 calendar days, after which time the Solution will be moved to the SPoC Solution Expired List. A full Evaluation (including applicable fees) is required to return the Solution Listing status to good standing.

Upon receipt of the updated AOV and any applicable documentation, PCI SSC will do the following:

1. Review the submission for completeness.
2. When completeness is established, sign and return a copy of the updated AOV to the Solution Provider and SPoC Lab.
3. Update the annual checkpoint date on the Website.

5.2 Changes to SPoC Solution Listings

SPoC Solution Providers may update listed Solutions for various reasons, such as the addition of supported SCRP devices or PIN CVM Applications. Changes do not have any impact on reevaluation dates of Solution Listings (Solution expiry dates or annual checkpoint dates). Table 2 describes the change types for listed Solutions and supported Solution Elements.

Note: *Adding support for a major version of a COTS operating system may be considered high impact or may be considered as a Delta change, as determined by the SPoC Lab. The SPoC Lab must carefully examine the security relevant changes in the SPoC Solution and the impact it has on the original evaluation outcome. The SPoC Lab may address queries (e.g., clarifications) to PCI SSC prior to submitting the SPoC Evaluation Report.*

Table 2: Changes to Listed Solutions

Change Type	Description
Administrative	Changes made to a listed Solution that have no impact on compliance with any of the *SPoC Security Requirements*, but where the List of Validated SPoC Solutions is updated to reflect the change. Examples of administrative changes include, but are not limited to, corporate identity changes and changes to Listing details, such as "Description." For details, see Section 5.2.1, *Administrative Changes for SPoC Solution Listings*.
No impact Change	Any change that does not impact security functions or compliance with the *SPoC Standard,* such as maintenance patches or routine key rotation. No impact Changes are not reported in detail but are addressed by the Solution Provider during the annual checkpoint.
Delta Change	Limited to non-high-impact changes where the SPoC Lab determines that the change has a low security risk or has a low impact on compliance with the *SPoC Standard*, for example*:* • Add/remove a PCI SSC-approved SCRP, MSR approved under the PCI PTS program with SCR Approval Class, or non-PTS approved MSR validated by a SPoC Lab (per the *SPoC MSR Annex*) for use in the Solution • Add/remove a validated PIN CVM Application (or optional SPoC API) • Update a validated PIN CVM Application Delta Changes can be assessed separately; that is, a full Evaluation is not required to validate the change. For details, see Section 5.2.2, *Delta Changes*.
High impact Change	High impact Changes are changes where the SPoC Lab determines that the extent of the change has a high security risk or a significant impact on the overall SPoC Solution; a full Evaluation of the SPoC Solution is required. High impact Changes are not reported in a Change Impact template because they require a full Evaluation (see Section 4, *Evaluation and Reporting Processes* for details). ***Note:*** *Adding support for a major version of a COTS operating system may be considered as high impact by a SPoC Lab. It is up to the SPoC Lab to determine.* *Adding support for a different COTS platform (e.g., Android, iOS, etc.) is considered high impact, and therefore requires a full Evaluation of the SPoC Solution.* For details, see Section 5.2.3, *High impact Changes*.

5.2.1 Administrative Changes for SPoC Solution Listings

Administrative Changes are limited to updates where no changes to a Listed SPoC Solution have occurred, but the Solution Provider wishes to request a change to the way that the Solution is Listed on the Website. For details about the content of the change analysis, see Section 5.3, *Change Documentation*.

Note: *Administrative Changes are permissible only for Listed Solutions that have not expired.*

The Solution Provider prepares a change analysis using the Change Impact template (*Appendix C*) and submits it to the SPoC Lab for review. At a minimum, the change analysis must contain the following information:

- Name and reference number of the Validated SPoC Solution Listing
- Description of the change
- Description of why the change is necessary

The Solution Provider should submit the change analysis to the same SPoC Lab that performed the original SPoC Solution Evaluation, as changing SPoC Labs requires a full Evaluation of the Solution. If the SPoC Lab agrees that the change is eligible as an Administrative Change:

1. The SPoC Lab notifies the Solution Provider that the change is eligible.
2. The Solution Provider prepares the change documentation, signs the corresponding AOV, and sends the documentation to the SPoC Lab.
3. If applicable, the Solution Provider completes a new VRA.
4. The SPoC Lab completes the change documentation and signs the AOV.
5. The SPoC Lab signs its concurrence on the AOV and forwards it, along with the change documentation (and new VRA if applicable) to PCI SSC.
6. PCI SSC sends the Change Fee invoice to the Solution Provider.
7. Upon payment of the invoice, PCI SSC reviews the submission.

If the SPoC Lab does not agree that the change is eligible as an Administrative Change, the SPoC Lab works with the Solution Provider to resolve the disagreement.

Following a successful PCI SSC review of the change, PCI SSC:

1. Updates the corresponding List of Validated SPoC Solutions on the Website accordingly with the new information.
2. Signs and returns a copy of the corresponding AOV to the Solution Provider and the SPoC Lab. The Revalidation date of the updated Listing remains the same as that of the parent Listing.

Should there be quality issues with any part of the submission, PCI SSC will communicate them to the SPoC Lab. PCI SSC reserves the right to reject any change submission if it determines that the change is ineligible as an Administrative Change.

5.2.2 Delta Changes

Delta Changes are changes made to a SPoC Solution, PIN CVM Application and/or supporting Monitoring/Attestation System and are limited to changes where the SPoC Lab determines that a partial Evaluation (Delta Evaluation) can be performed, rather than a full Evaluation of the SPoC Solution. For example, addition/removal of a validated SCRP device, MSR approved under the PCI PTS program with SCR Approval Class, or non-PTS approved MSR (per the SPoC MSR Annex) used in a Solution, addition/removal or changes to the PIN CVM Application that only impact the tamper-protection features, adding/removing support for a major version of a COTS operating system may be eligible for Delta Evaluation.

Since the number of possible changes and their impact cannot be determined in advance, the type of Evaluation must be considered on a per-case basis. Solution Providers should contact the SPoC Lab that performed the last full Solution Evaluation for guidance. The SPoC Lab engaged by the Solution Provider for this purpose then determines whether a Delta Evaluation or full Evaluation is required based on scope of the changes and the impact on the security and/or SPoC-related functions of the SPoC Element, the impact to *SPoC Standard* and/or the scope of the changes being made. See Section 5.3, Change Documentation.

The Solution Provider prepares a change analysis using the Change Impact template (*Appendix C*) and submits it to the SPoC Lab for review. At a minimum, the change analysis must contain the following information:

- Name and reference number of the Validated SPoC Solution Listing
- Description of the change
- Description of why the change is necessary

The Solution Provider should submit the change analysis to the same SPoC Lab that performed the previous full Evaluation, as changing SPoC Labs requires a full Evaluation of the SPoC Solution. If the SPoC Lab does not agree that the change is eligible as a Delta Change, the SPoC Lab works with the Solution Provider to resolve the disagreement.

If the SPoC Lab agrees that the change is eligible as a Delta Change:

1. The SPoC Lab notifies the Solution Provider that the change is eligible,
2. The Solution Provider prepares the change documentation and signs the AOV (and new VRA, if applicable) and sends it to the SPoC Lab,

3. The SPoC Lab completes the Change Impact document and produces a red-lined Evaluation Report and documents the testing completed per PCI SSC requirements,
4. The SPoC Lab signs its concurrence on the AOV and forwards it with the completed change documents, VRA (if applicable), and the red-lined Evaluation Report to PCI SSC,
5. PCI SSC sends a Change Fee invoice to the Solution Provider,
6. Upon payment of the invoice, PCI SSC reviews the submission.

Following a successful review of the change, PCI SSC does the following:

1. Amends the List of Validated SPoC Solutions on the Website with the new information.
2. Signs and returns a copy of the AOV to the Solution Provider and the SPoC Lab. The Revalidation date of the updated Listing remains the same as that of the parent Listing.

Should there be quality issues with any part of the submission, PCI SSC communicates them to the SPoC Lab. PCI SSC reserves the right to reject any submission if it determines that a change described therein and purported to be a Delta Change by the SPoC Lab or Solution Provider is ineligible for treatment as a Delta Change.

5.2.3 High impact Changes

High impact Changes are those affecting a SPoC Solution, PIN CVM Application and/or supporting Monitoring/Attestation System where the SPoC Lab determines that the magnitude of the change is greater than what can be validated by a Delta Evaluation. Therefore, a full Evaluation of the entire SPoC Solution is necessary. For example, a High impact Change might impact multiple modules of the *SPoC Standard* and cannot be tested or validated separately from the Solution. High impact Changes are not reported in a Change Impact template because they require a full Evaluation (see Section 4, *Evaluation and Reporting Processes*).

Because the number of possible changes and their impact cannot be determined in advance, the type of Evaluation must be considered on a per-case basis. Solution Providers should contact the SPoC Lab that performed the last full Solution Evaluation for guidance. The SPoC Lab engaged by the Solution Provider for this purpose determines whether a full Evaluation is required based on the scope of the changes being made, the impact to the *SPoC Standard* and/or the degree to which the change impacts the security and/or SPoC-related functions.

Note: *Updating a SPoC Solution to support a new/major version of a COTS device operating system (for example, from version 9.x to version 10.x) may be considered high impact by the SPoC Lab, and therefore may require a full Evaluation of the SPoC Solution. It is the responsibility of the SPoC Lab to determine the scope of the change's impact on the overall SPoC Solution, to and* *determine whether a full Evaluation must be performed, or if the change can be validated via delta Evaluation.*

Note: *Updating a SPoC Solution to support a different COTS platform (e.g., Android, iOS, etc.) is considered high impact, and therefore requires a full Evaluation of the SPoC Solution.*

5.3 Change Documentation

Table 3 summarizes the change documentation.

Table 3: Change Documentation

Administrative Change	Delta Change	Annual Checkpoint
• Solution Attestation of Validation (AOV) • Change Impact document [a] • Current VRA [b] • Fee	• Solution Attestation of Validation (AOV) • Change Impact document [a] • Red-lined Evaluation Report • Current VRA [b] • Fee	• Solution Attestation of Validation (AOV) • Red-lined Evaluation Report • Solution Provider's Back-end Environment AOC(s) [b] • Current VRA [b]

[a] The *Change Impact* document in Appendix C is mandatory for the SPoC Lab when submitting changes to PCI SSC on behalf of Solution Providers.

[b] If applicable.

5.4 Acceptance and Change Fees

Note: *The Solution Provider pays all SPoC Solution Evaluation fees directly to the SPoC Lab. The SPoC Lab and the Solution Provider negotiate these fees. PCI SSC sends an invoice to the Solution Provider for all Acceptance and change fees, and the Solution Provider pays these fees directly to PCI SSC.*

Prior to Acceptance, the Solution Provider must pay the applicable Acceptance Fee to PCI SSC. For any change affecting the validated SPoC Solution, the invoiced Change Fee must be received by PCI SSC before the change will be reviewed. Upon Acceptance, PCI SSC signs and returns a copy of the *AOV* to the Solution Provider and the SPoC Lab and updates the List of Validated SPoC Solutions.

There is no PCI SSC fee for processing of annual checkpoints. All SPoC Program fees are posted on the Website (see Fee Schedule). SPoC Program fees are non-refundable and are subject to change upon posting of revised fees on the Website.

5.5 Renewing Expiring Listings

As a Solution Listing approaches its Reevaluation Date (expiry date), PCI SSC will notify the Solution Provider of the pending expiration. The two options are available to the Solution Provider:

- **New Validation:** If the Solution Provider wants the Solution Listing to remain on the List of Validated SPoC Solutions, the Solution Provider must engage a SPoC Lab to perform a new full Evaluation. The SPoC Lab performs the Evaluation against the current *SPoC Standard* before the expiry date, resulting in a new Acceptance. A new Evaluation follows the same process as the original SPoC Solution Evaluation.
- **Expiry:** A Solution Listing for which a new Acceptance has not occurred on or before the expiry date appears in **Orange** for the first 90 days past expiry.
  - If the SPoC Solution undergoes a full reevaluation and the submittal is received by PCI SSC within this 90-day period, PCI SSC will update the corresponding Listing's Reevaluation date with the new date and remove the **Orange** status.
  - If the SPoC Solution is not reevaluated and submitted to PCI SSC within this 90-day period, the corresponding Listing's Reevaluation date will be updated to show the date in **Red** for a period of no longer than 90 calendar days, after which time the Solution will be moved to the SPoC Solution Expired List. A full Evaluation (including applicable fees) is required to return the Solution Listing status to good standing.

Note: *If an OS becomes unsupported by the OS vendor after the initial Evaluation, it can continue to be used until an annual checkpoint. As part of the annual checkpoint, the SPoC Lab* *performs additional testing to confirm security objectives outlined in the SPoC Unsupported OS Annex are met, and that the use of such a platform will not increase PIN exposure or subversion of the payment process.*

If evaluation per the SPoC Unsupported OS Annex is not performed or the implemented security controls and processes are not accepted by the SPoC Lab, the SPoC Standard requires (Security Requirement 4.3.7) that merchants who are using the PIN CVM Application on affected platforms be notified by the SPoC Solution Provider, and the listed SPoC Solution will be shown on the Website listing as expired within the Solution Details portion of the SPoC listing.

5.6 Validation Maintenance Fees

If a Listed Solution is revised, the Solution Provider is required to pay the applicable change fee to PCI SSC. To accept and list a change, a Solution must already be listed and not have reached the expiry date.

For any change affecting the List of Validated SPoC Solutions, the invoiced fee must be received by PCI SSC before the change can be reviewed, accepted, and added to the List of Validated SPoC Solutions. Upon acceptance, PCI SSC signs and returns a copy of the AOV to the Solution Provider and the SPoC Lab.

There is no PCI SSC fee for processing annual checkpoints.

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

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

In the event of a security issue relating to a Validated SPoC Solution, the VRA requires the Solution Provider to notify PCI SSC. Solution Providers must be aware of and adhere to their obligations under the VRA in the event of a security issue.

6 Reporting Considerations

Per section 3.7, PCI SSC's secure website (Portal) is used by PCI SSC and SPoC Labs to track communications relating to a submission. For example, for any Solution to be listed on the Website, all documents relating to the validation of the corresponding candidate Solution are to be submitted by the applicable SPoC Lab, on behalf of the Solution Provider, to PCI SSC through the Portal.

6.1 Evaluation Report Acceptance, Issuance of Approval Overview

***Note:** PCI SSC review times are estimates and may vary based on workload and other factors.*

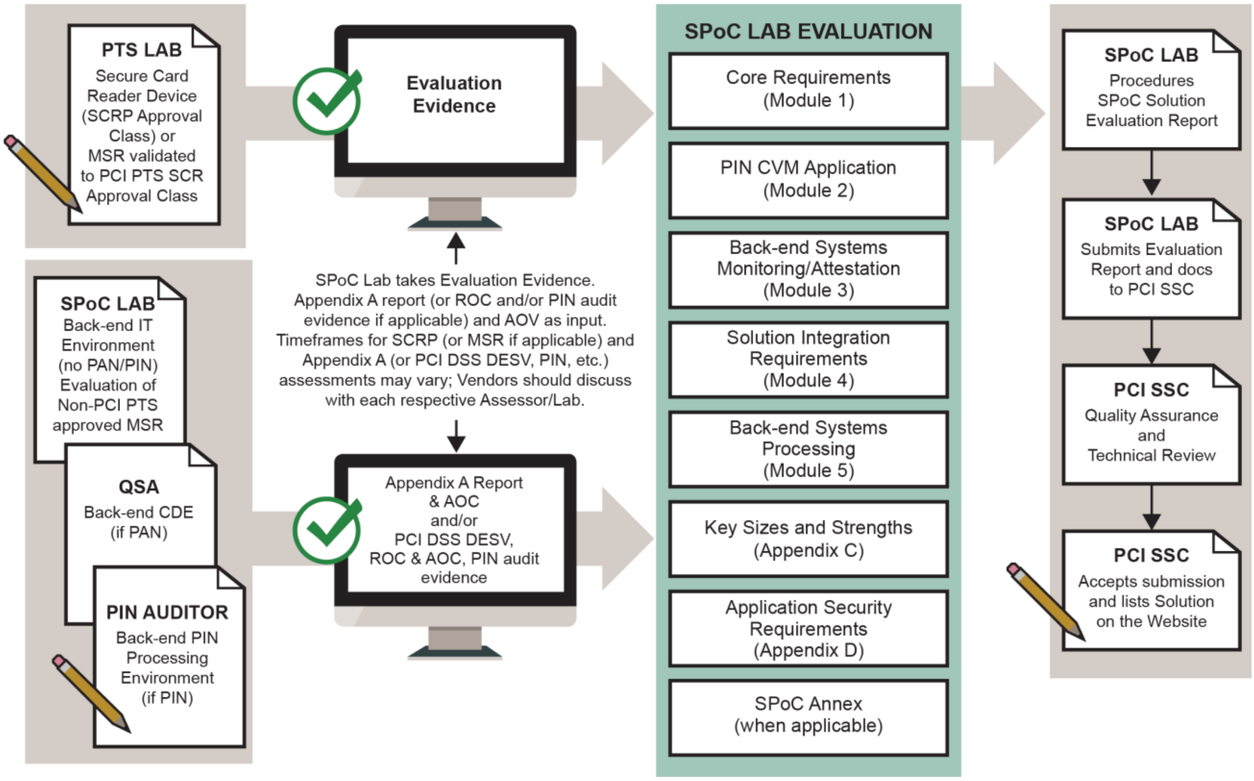
Upon receipt of the submission for a new SPoC Solution, PCI SSC identifies technical issues or questions for resolution by the SPoC Lab, typically within two calendar weeks of receipt. Subsequent SPoC Lab responses and information will be reviewed, and the cycle will repeat until satisfactory responses have been received or the submission is rejected or withdrawn.

When PCI SSC determines that there are no issues or questions, PCI SSC adds the Solution to the List of Validated SPoC Solutions and issues a countersigned AOV.

For reports on changes to existing Listed Solutions, such as Delta Changes, the same process applies. Upon determining that no issues or questions remain, PCI SSC posts revised information to the Website and issues a countersigned AOV. Delta reports are prepared using the same major requirements that were used during the original Solution Evaluation.

Figure 4 illustrates the SPoC Solution process including submission, SPoC Lab Evaluation, and PCI SSC review and Acceptance.

Figure 4: SPoC Solution Process


PTS LAB
Secure Card Reader Device (SCRP Approval Class) or MSR validated to PCI PTS SCR Approval Class
Evaluation Evidence
SPoC Lab takes Evaluation Evidence. Appendix A report (or ROC and/or PIN audit evidence if applicable) and AOV as input. Timeframes for SCRP (or MSR if applicable) and Appendix A (or PCI DSS DESV, PIN, etc.) assessments may vary; Vendors should discuss with each respective Assessor/Lab.
SPoC LAB
Back-end IT Environment (no PAN/PIN) Evaluation of Non-PCI PTS approved MSR
QSA
Back-end CDE (if PAN)
PIN AUDITOR
Back-end PIN Processing Environment (if PIN)
Appendix A Report & AOC and/or PCI DSS DESV, ROC & AOC, PIN audit evidence
SPoC LAB EVALUATION
Core Requirements (Module 1)
PIN CVM Application (Module 2)
Back-end Systems Monitoring/Attestation (Module 3)
Solution Integration Requirements (Module 4)
Back-end Systems Processing (Module 5)
Key Sizes and Strengths (Appendix C)
Application Security Requirements (Appendix D)
SPoC Annex (when applicable)
SPoC LAB
Procedures SPoC Solution Evaluation Report
SPoC LAB
Submits Evaluation Report and docs to PCI SSC
PCI SSC
Quality Assurance and Technical Review
PCI SSC
Accepts submission and lists Solution on the Website

6.2 Delivery of the Evaluation Report and Related Materials

To list a Solution on the Website, the SPoC Lab (on behalf of the Solution Provider) must submit all Solution-validation-related documents to PCI SSC through PCI SSC's secure website (Portal). PCI SSC pre-screens the submissions in the Portal to ensure that all required documentation has been included, and the basic submission requirements have been satisfied.

Information in the submitted documents must be consistent with the entries in the "Details" fields within the Portal. Common submission errors include inconsistent product names or contact information and incomplete or inconsistent documentation. Ineligible, incomplete or inconsistent submissions may delay processing of Listing requests or result in the rejection of the submission by PCI SSC.

6.2.1 Resubmissions

For subsequent reviews, if an Evaluation Report requires multiple iterations before PCI SSC accepts the report, each report that the SPoC Lab submits must track cumulative changes.

6.3 Quality Management Programs

Assessors and SPoC Labs must meet all quality assurance standards set by PCI SSC that apply to the SPoC Program. SPoC Labs, QSA Companies and PCI QPA Companies are subject to all quality assurance policies, procedures, and requirements of the PTS Program, QSA Program and QPA Program as described in their respective Program documents (for example, Program Guides, Qualification Requirements, Agreements).

6.3.1 Evaluation Report Submission Review

PCI SSC reviews each Evaluation Report after the Solution Provider pays the acceptance fee. PCI SSC first screens the submission to ensure that it is complete. If the submission is complete, PCI SSC reviews the submission in its entirety.

PCI SSC reviews the submission to determine whether the candidate Solution is eligible for validation pursuant to SPoC Program requirements, including but not limited to the *Program Guide*. If there is eligibility question, PCI SSC contacts the SPoC Lab for additional information. If the candidate Solution is ineligible for validation under the SPoC Program, the Evaluation Report is rejected and the SPoC Lab will receive a letter of rejection with instructions for appeal.

If the candidate Solution is eligible for validation under the SPoC Program, PCI SSC conducts a complete review of the Evaluation Report and supporting documentation provided or subsequently requested by PCI SSC. Any comments or feedback from PCI SSC will be made through the Portal. The SPoC Lab should address all comments and feedback in a timely manner. PCI SSC's role is to ensure that the SPoC Solution Evaluation was performed in accordance with SPoC Program requirements and quality standards.

Appendix A SPoC Program Acceptance

Acceptance of a given SPoC Solution or SPoC Element by PCI SSC applies only to the specific SPoC Solution or SPoC Element that has been validated by a SPoC Lab and subsequently Accepted by PCI SSC (each an Accepted Element). If any aspect of a SPoC Solution or SPoC Element is different from that which was validated by the SPoC Lab and Accepted by PCI SSC—even if the different SPoC Solution or SPoC Element (each an "Alternate Element") conforms to the basic product description of the Accepted Element—the Alternate Element should not be considered Accepted by PCI SSC, nor promoted as Accepted by PCI SSC.

No SPoC Solution Provider or other third party may refer to a SPoC Solution or SPoC Element as "PCI Approved," or "PCI SSC Approved" or otherwise state or imply that PCI SSC has, in whole or part, approved any aspect of a SPoC Solution Provider or its SPoC Solution or SPoC Element, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with PCI SSC, or in a corresponding AOV provided by PCI SSC. All other references to PCI SSC's acceptance of a SPoC Solution or SPoC Element are strictly and actively prohibited by PCI SSC.

When granted, PCI SSC Acceptance is provided to ensure certain security and operational characteristics important to the achievement of PCI SSC's goals, but such acceptance does not under any circumstances include or imply any endorsement or warranty regarding the applicable SPoC Solution Provider or the functionality, quality or performance of the SPoC Solution or SPoC Element or any other product or service. PCI SSC does not warrant any products or services provided by third parties. PCI SSC acceptance does not, under any circumstances, include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services that have received acceptance from PCI SSC shall be provided by the party providing such products or services, and not by PCI SSC or any Participating Payment Brand.

Appendix B Elements for the List of Validated SPoC Solutions

Field	Description
Company	The SPoC Solution Provider for the validated Solution.
Solution Name, Solution version	Name supplied by the SPoC Solution Provider under which the Solution is sold. This field also includes the version of the SPoC Solution, provided by the SPoC Solution Provider
Reference Number	A number assigned by PCI SSC when the validated Solution is posted to the Website. This number is unique per SPoC Solution Provider and SPoC Solution and remains the same for the life of the Listing. An example reference number is 2021-XXXXX.XXX, consisting of the following: • Year of Listing—4 digits + hyphen • Solution Provider #—5 digits + period (assigned alphabetically initially, then as received) Individual Solution Number #—3 digits
SPoC Version	The version of the *SPoC Standard* used to evaluate and validate Solution compliance
Evaluation Lab	The name of the SPoC Lab that performed the Evaluation and validated that the Solution is compliant with all applicable SPoC Security Requirements.
Reevaluation Date	The date by which the Solution Provider must have the Solution fully re-evaluated and validated against the current *SPoC Standard* to maintain the Acceptance. **Orange**- or **Red**-colored indicators next to this field signify that the Solution is overdue for submittal to PCI SSC.
Annual Checkpoint Due	The date that the Solution is due for its 12- and 24-month checkpoints by a SPoC Lab. **Orange**- or **Red**-colored indicators by this field signify that the Solution is overdue for submittal to PCI SSC.

Field	Description
Solution Details (hyperlink)	Clicking on this link brings up a list of details specific to this Solution consisting of the following: – **SCRP Devices Supported**: Identifies the PCI SSC-approved SCRP devices validated for use with this Solution and will include relevant PCI PTS reference numbers and the expiry date of the PTS approval for this device. If the expiry date is in the past, this will be denoted by a color change. A website link will be provided to the appropriate entry on the PCI PTS Approved Device List on the Website. – **MSRs Supported:** Identifies the PTS-approved or non-PTS approved MSR that has been validated by the SPoC Lab for use with the Solution, and the expiry date of the approval for this device. If the expiry date is in the past, this will be denoted by a color change. If the device is PTS-approved, a link will be provided to the appropriate entry on the PCI PTS Approved Device List on the Website. The Expiry date for a non-PTS approved MSR is the same as the expiry date of the SPoC Solution in which that non-PTS approved MSR is incorporated, and the non-PTS approved MSR must be re-evaluated each time the SPoC Solution is re-evaluated. – **PIN CVM Application(s) Evaluated:** Identifies the PIN CVM Application validated for use with this Solution: ○ Application: PIN CVM Application name and version ○ OS: Operating system(s) on which the application was tested and validated ○ OS Version(s): Major version of the operating system on which the application was tested and is supported. – **SPoC API(s) Evaluated:** Identifies the optional SPoC API validated for use with this Solution: ○ SPoC API: SPoC API name and version ○ OS: Operating system(s) on which the SPoC API was tested and validated ○ OS Version(s): Major version of the operating system on which the SPoC API was tested and is supported. *Note that while a SPoC Solution or SPoC Element may include third-party services (including services such as KIFs), those are not listed within the Solution. Any use of such service in another SPoC Solution would require Evaluation as part of each SPoC Solution of which the third-party service is a part.*

Appendix C Change Impact Template for SPoC Solutions

This *SPoC Change Impact Template* is required for Administrative Change and Delta Change submissions to SPoC Solutions or SPoC Elements (for example, a PIN CVM Application or supporting Monitoring/Attestation System). Refer to the *SPoC Program Guide* for information about any SPoC Solution Listing changes.

The Solution Provider and/or SPoC Lab must complete each applicable section of this document and all other required documents based on the type of change (see *Table 2*). The SPoC Lab submits this *SPoC Change Impact* form with supporting documentation to PCI SSC for review.

Part 1. SPoC Solution Listing Details, Contact Information and Change

SPoC Solution Listing Details			
SPoC Solution Name		Validated Listing Reference Number	
Type of Change *(check one)*	□ Administrative *(Complete Part 2)*	□ Delta *(Complete Part 3)*	
Submission Date			

Solution Provider Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	
SPoC Lab 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 Solution Provider Company Name		Revised Solution Provider Company Name *(if applicable)*	
Current SPoC Solution or PIN CVM Application Name		Revised SPoC Solution or PIN CVM Application Name *(if applicable)*	
Additional details, as applicable			

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

For each change that is eligible for Delta Evaluation, identify the type of change applicable to this submission and complete the applicable sections of this SPoC Change Impact form (check all that apply). Changes that impact compliance with the *SPoC Standard* must be reflected in the submitted red-lined *Evaluation Report*.

Use additional rows or add pages if needed.

Delta Change Revision			
Refer to the *SPoC Program Guide* for details about each type of change.			
Add/remove SCRP Device *(Complete Part 3a)*	□ Add	□ Remove	
Add/remove MSR *(Complete Part 3a-1)*	□ Add	□ Remove	
Add/change/remove PIN CVM Application or SPoC API *(Complete Part 3b)*	□ Add	□ Change	□ Remove
Other Delta Change not listed above *(Complete Part 3c)*	□ [type of change - to be filled in by Solution Provider or SPoC Lab]		
Detailed description of changes to the SPoC Solution			
Detailed description of how the change impacts the SPoC Solution’s security or functionality			
Description of how the change is reflected in the Solution Provider’s versioning methodology, if applicable, including how this version number indicates the type of change			
Additional details, as applicable			

Part 3a. Add/Remove SCRP Device Type (if indicated at Part 3)

SCRP Device Type		
Adding for inclusion in Listing or removal from Listing?	□ Addition/Inclusion in Listing *(Red-lined Evaluation Report review required, see details below)*	□ Removal from Listing *(No Red-lined Evaluation Report review required)*
SCRP Device type name/identifier		
SCRP Device manufacturer, model and number		
PTS approval number for SCRP Device		
SCRP Device Hardware version #		
SCRP Device Firmware version #		
Notes/details (if applicable)		

Generate a red-lined Evaluation Report for the added device(s).

Part 3a-1. Add/Remove MSR (if indicated at Part 3)

Magstripe Reader Type		
Adding for inclusion in Listing or removal from Listing?	□ Addition/Inclusion in Listing *(Red-lined Evaluation Report review required, see details below)*	□ Removal from Listing *(No Red-lined Evaluation Report review required)*
MSR type name/identifier		
MSR manufacturer, model and number		
PTS approval number for MSR (if applicable)		
MSR Hardware version #		
MSR Firmware version #		
Notes/details (if applicable)		

Generate a red-lined Evaluation Report for the added device(s).

Part 3b. Add/Change/Remove PIN CVM Application (or API) (if indicated at Part 3)

PIN CVM Applications (or API)			
Adding or changing Listing, or removal from Listing?	□ Addition or change in Listing *(Red-lined Evaluation Report review required, see details below)*	□ Removal from Listing *(No Red-lined Evaluation Report review required)*	
Current PIN CVM Application Name		Revised PIN CVM Application Name *(if applicable)*	
Current PIN CVM Application Version		Revised PIN CVM Application Version *(if applicable)*	
Operating system(s) currently tested and validated to support. Include major OS version (e.g., 10.x)		Updated operating system(s) tested and validated to support	
Description of the purpose for this change			
Notes/details (if applicable)			

Generate a red-lined Evaluation Report for the changes to the SPoC PIN CVM Application or SPoC API (if applicable).

Part 3c. Other Delta Change (if indicated at Part 3)

Other Delta Change	
Description of the change	
Description of the purpose for this change (if not included above)	
Additional details, Solution Provider or SPoC Lab notes, etc., as applicable	

Generate a red-lined Evaluation Report for the change.

Appendix D SPoC Solution Provider-offered Libraries or APIs

In cases where the SPoC Solution Provider provides an application programing interface (API) or libraries to allow third parties to interface the Solution Provider's SPoC Solution, the following requirements must be met:

- The SPoC Solution Provider is responsible for the development and validation of the SPoC API and a companion document ("user guidance") outlining the conditions and how the SPoC API can be used to interface the SPoC Solution.
    - The user guidance describes the scope of integration, any reporting obligations to PCI SSC, review periods, actions on changes, updates, resource management, distribution process, etc.
    - The SPoC Solution Provider is responsible for all terms and conditions in the user guidance and must submit the user guidance to the SPoC Lab as part of each SPoC Solution Evaluation (or applicable change submittal) for which a SPoC API is provided.
    - The SPoC Solution Provider must make the user guidance available to all third parties that interface the SPoC Solution via the provided API.
- The SPoC Lab must assess the SPoC API (and any associated software) and the companion user guidance as part of each applicable SPoC Solution Evaluation, and each applicable change submittal.
    - The SPoC Lab must validate that usage of the SPoC API (e.g., integration of a user interface or business logic with a SPoC Solution) in conjunction with the SPoC Solution does not cause the SPoC Solution to violate or be noncompliant with any of the SPoC security requirements by the SPoC Solution.
    - The SPoC API will be listed under the SPoC Solution Details page in the List of Validated SPoC Solution.

- The SPoC Solution Provider is accountable for managing all API-related changes (i.e., change impact, versioning, SPoC Lab integration testing and validation, etc.) including those changes made by third parties that utilize the API. For example, if a third party develops and manages their own user interface to interface the SPoC Solution via the Solution provider's API, it must not be possible for changes to the third party user interface to impact compliance of the Solution or SPoC API with any of the SPoC security requirements. The SPoC Solution Provider is responsible for the Solution's security including any impactful changes.

***Note:** Any change to the SPoC Solution that requires the code to be recompiled (in order to accommodate the change) requires an update to the Solution's Listing. See section 5.2 for additional details on changes to SPoC Solutions.*

If a SPoC Solution Provider optionally provides a SPoC API to allow third parties to interface the listed SPoC Solution, the SPoC API is part of *only* the SPoC Solution with which it was Evaluated, validated and listed on the PCI SSC Website. Third parties are not permitted to reuse the SPoC API as part of another SPoC Solution without separate validation by a SPoC Lab.

Appendix E Software Versioning Methodology

Changes to production-level code necessitate updates to the respective software application's version numbering. Solution Providers must document and follow a software-versioning method as part of their system development lifecycle; the software-versioning method may be a separate document or part of the Solution Provider's security policy. Additionally, PIN CVM Application vendors must communicate the versioning method to their customers and integrators/resellers in their implementation guidance documents. Customers and integrators/resellers require this information to understand what version of the application they are using and the changes to each version. As part of the SPoC Evaluation, SPoC Labs must verify that the Solution Provider adheres to the versioning method and the requirements of the *SPoC Program Guide*. If the Solution Provider maintains a separate, internal version-numbering scheme, the Solution Provider must document and maintain a method to accurately map the internal version numbers to the publicly listed version numbers.

For additional information, see the *SPoC Standard*, Appendix D, "Application Security Requirements," (item 9).

Version Number Format

The Solution Provider sets the application version number format, which may be comprised of several elements. The versioning method must fully describe the application version number format, including the following:

- Version scheme format
  - Number of elements
  - Numbers of digits for each element
  - Format of separators between elements
  - Character set for each element (alphabetic, numeric, alphanumeric)
- Element hierarchy
  - Definition of each element in the version scheme
  - Type of change: major, minor, or maintenance release, and so on

Version Number Usage

All Delta and high impact changes[1] to the PIN CVM Application (and/or its Monitoring/Attestation System) must result in a new application version number. All changes that impact security functions and/or any SPoC Security Requirements must result in a change to the version number listed on the PCI SSC Website.

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

- Types of changes made to the application, such as major release, minor release, maintenance release, and so on
- Changes that have no impact on the function of the application or its dependents
- Changes that impact the application function, but do no impact security or compliance with the *SPoC Standard*
- Changes that impact any security function or compliance with the *SPoC Standard*

Elements of the version number used for changes that do not impact security functions must never be used for changes that do impact security functions.

If the Solution Provider 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 integrators/resellers must be consistent with the versioning policy described in the applicable implementation guides.

Solution Providers must ensure traceability between application changes and version numbers. Customers and integrators/resellers must be able to determine what changes are included in the version of the application they are running.

[1] See *Table 2* for an overview of the various change types.

Appendix F Terminology

Table 4 lists the terms used in this *Program Guide* and their meanings. Terms not listed in Table 4 may be found in the documents listed in Section 1.2, *Related Publications* (each document is available on the Website).

Table 4: PCI SSC Terminology

Term	Definition / Source / Document Reference
Accepted/Acceptance	A SPoC Solution is deemed to have been "Accepted" (and "Acceptance" is deemed to have occurred) and will be listed on the List of Validated SPoC Solutions on the Website when PCI SSC has: • Received the corresponding compliant Solution Evaluation Report from the SPoC Lab; • Received the corresponding fee and all documentation required with respect to that SPoC Solution as part of the SPoC Program; and • Confirmed that: – The respective compliant Solution Evaluation Report is correct as to form (all applicable documents completed); – The SPoC Lab determined that the Solution is eligible to be a validated Solution; – The SPoC Lab reported the compliance of the respective SPoC Solution with SPoC Program requirements; and – The detail provided in the Solution Evaluation Report meets PCI SSC's reporting requirements. ***Note:*** *PCI SSC may suspend, withdraw, revoke, cancel or place conditions upon (including without limitation, complying with remediation requirements) Acceptance and Listing of any Solution in accordance with applicable SPoC Program policies and procedures.*
Assessment	Assessment of a SPoC Solution's Back-end Monitoring Environment to validate compliance with the *SPoC Standard* as part of the SPoC Program.
Assessor	A SPoC Lab or a QSA company or a PCI QPA.
AOV	Acronym for "Attestation of Validation." As applicable to the SPoC program, the AOV is a form for SPoC Labs and SPoC Solution Providers to attest to the results of a SPoC Evaluation, declaring the SPoC Solution validation status against the *SPoC Standard*. The AOV, signed by the SPoC Lab and Solution Provider, is used when validating, revalidating or submitting changes to a Solution.
AOC	Acronym for "Attestation of Compliance." As applicable to PCI DSS validation, the AOC is a form for merchants and service providers to attest to the results of a PCI DSS assessment. As applicable to PCI PIN validation, the AOC is a form for merchants and service providers to attest to the results of a PCI PIN assessment.
Back-end Monitoring Environment	The secure facility or environment assessed by a SPoC Lab (or QSA Company or PIN auditor, as applicable) in accordance with the *SPoC Standard* Appendix A, "Monitoring Environment Basic Protections," which includes (but is not limited to) network infrastructure, physical and logical security controls, access controls, vulnerability management and governance and security policies in which a Monitoring/Attestation System is hosted.

Term	Definition / Source / Document Reference
COTS	Acronym for commercial off-the-shelf [device].
DESV	Acronym for Designated Entities Supplemental Validation. See the *PCI Glossary* for additional information.
Delta Evaluation	Partial Evaluation of the Solution, performed against applicable SPoC Security Requirements, when changes to a Solution are eligible for review under the "Delta Evaluation" change-review process described herein.
Evaluation	See *SPoC Solution Evaluation.*
Evaluation Report	The SPoC Solution Evaluation Report required to be completed by a SPoC Lab during SPoC Solution Evaluations and submitted to PCI SSC for review and Acceptance, following the SPoC Solution Evaluation Report Template (available on the Website) and instructions therein. For a Solution to be included on the List of Validated SPoC Solutions on the Website, the corresponding Evaluation Report must be submitted to PCI SSC for review and Accepted.
List of Validated SPoC Solutions	The list of SPoC Solutions on the Website that have been Accepted for SPoC Program purposes.
Listing (or Listed)	The listing and related information regarding a Solution on the List of Validated SPoC Solutions.
MSR	Acronym for Magnetic Stripe Reader (or Magstripe Reader). See *SPoC MSR Annex* for details.
Monitoring/Attestation System	An application which includes any COTS device-side and back-end monitoring and/or attestation software applications that has been evaluated and validated by a SPoC Lab to have met all applicable SPoC Security Requirements, and then Accepted by PCI SSC, so long as such Acceptance has not been revoked, suspended, withdrawn, or terminated. In the *SPoC Standard*, the Monitoring/Attestation System is an implementation that may be shared across different execution environments and which provides a level of validation and assurance of the execution environment in which the PIN CVM Application executes, thereby delivering a level of software-based tamper detection and response.
Non-PTS approved MSR	A Magnetic Stripe Reader that has *not* undergone evaluation and approval by a PTS Lab in accordance with the PCI PIN Transaction Security POI Standard. Non-PTS approved MSRs are *not* listed on the PCI PTS Approved Device list.
Participating Payment Brand (or Payment Brand)	A payment card brand that, as of the time in question, is then formally admitted as (or an affiliate of) a member of PCI SSC pursuant to its governing documents. *Note: At the time of this publication, Participating Payment Brands include PCI SSC's Founding Members and Strategic Members.*
PAN	Acronym for Primary Account Number.
PCI PTS Approved Device list	The list of PCI PTS-Approved PIN Transaction Security Devices which is currently available at https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
PCI SSC	Acronym for PCI Security Standards Council, LLC.
PIN	Acronym for Personal Identification Number.
PIN CVM	Acronym for Personal Identification Number Cardholder Verification Method.

Term	Definition / Source / Document Reference
PIN CVM Application	All parts of the code, regardless of execution environment, that are installed and executed on the merchant COTS device for the purposes of accepting and processing the cardholder's PIN. See the *SPoC Standard* for additional details.
Program Guide	The then-current version of (or successor documents to) this document—the *Payment Card Industry (PCI) Software-based PIN Entry on COTS (SPoC) Program Guide,* as from time to time amended and made available on the Website.
PTS Program	The PCI SSC PIN Transaction Security program.
PTS Lab (or PCI-recognized Laboratory)	A security laboratory qualified by PCI SSC under the PCI SSC PCI-recognized Laboratory program.
Qualified PIN Assessor (QPA or PCI QPA)	QPA Company as defined in the *QPA Qualification Requirements* and qualified by PCI SSC to validate an entity's compliance with the PCI PIN Standard.
Qualified Security Assessor (QSA)	A QSA Employee or QSA Company as defined in the *QSA Qualification Requirements*.
QSA Company	A company then qualified by PCI SSC as a Qualified Security Assessor Company.
QSA Program	Defined in the *QSA Qualification Requirements*.
QSA Qualification Requirements	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Qualification Requirements for Qualified Security Assessors (QSA)*, as from time to time amended and made available on the Website.
SAD	Acronym for Sensitive Authentication Data.
SCRP	Acronym for Secure Card Reader – PIN. A physical card reader that has been assessed compliant to the PCI PTS SCRP Approval Class and is listed on the PTS approval website. See the *SPoC Standard* for additional details.
SPoC Application Programming Interface (or SPoC API)	An optional software component or libraries, developed and provided by the SPoC Solution Provider, to allow third-party developers to interface with the SPoC Solution.
SPoC Element	A PIN CVM Application, Monitoring/Attestation System, Back-end Monitoring Environment, SCRP or non-PTS Approved MSR, validated for use in a SPoC Solution.
SPoC Lab (or PCI-recognized SPoC Laboratory)	A PCI-recognized Software-based PIN Entry on COTS Laboratory qualified by PCI SSC to perform Evaluations of Solutions, PIN CVM Applications, supporting Monitoring/Attestation Systems and optional non-PTS Approved MSRs for SPoC Program purposes.
SPoC Program	PCI SSC's program and requirements for qualification of Assessors, Labs and applicable employees thereof and validation and Acceptance of SPoC Solutions or SPoC Elements, as further described in this document and related PCI SSC documents, policies and procedures.
SPoC Security Requirements	The then-current version of (or successor document(s) to) the *Payment Card Industry (PCI) Software-based PIN Entry on COTS Security Requirements*, any/all testing procedures, appendices, annexes, exhibits, schedules and attachments to the foregoing and all materials incorporated therein, in each case, as from time to time amended and made available on the Website.

Term	Definition / Source / Document Reference
SPoC Solution (or Solution)	The set of elements and processes that support software-based PIN entry on a COTS device, comprising a combination of validated SCRP(s), PIN CVM Application and supporting Monitoring/Attestation System, Back-end Monitoring Environment and related processes, which have been validated separately and as part of an integrated solution by the applicable SPoC Lab(s) and Accepted for Listing on the PCI SSC Website as part of the SPoC Program. At a minimum, a SPoC Solution must include at least one SCRP, a PIN CVM Application and supporting Monitoring/Attestation System and a Back-end Monitoring Environment.
SPoC Solution Evaluation (or Evaluation)	Evaluation of a Solution by a SPoC Lab for purposes of validating compliance against the *SPoC Standard* as part of the SPoC Program, including but not limited to: • Evaluation of the PIN CVM Application and supporting Monitoring/Attestation System incorporated therein • Testing and validation of the above with the applicable SCRP device • Testing and validation of the above with optional MSR(s), including evaluation of any non-PTS Approved MSRs used in the SPoC Solution • Back-end Monitoring Environment and all other elements of the Solution, and • End-to-end integration evaluation of the overall Solution.
SPoC Solution Expired List	The list of SPoC Solutions on the Website that have an expired status for a period of at least 90 days.
SPoC Solution Provider (or Solution Provider)	The provider of the overall SPoC Solution (or candidate Solution) – the SPoC Solution Provider is listed on the SPoC Solution Listing and ultimately accountable for the security and functionality of the SPoC Solution and its SPoC Elements.
SPoC Standard	The *SPoC Security Requirements* and *SPoC Test Requirements*, including any Annexes to the SPoC Standard as applicable.
SPoC Test Requirements	The then-current version of (or successor document(s) to) the *Payment Card Industry (PCI) Software-based PIN Entry on COTS Test Requirements*, any/all testing procedures, appendices, annexes, exhibits, schedules and attachments to the foregoing and all materials incorporated therein, in each case, as from time to time amended and made available on the Website.
SPoC user guidance document (or SPoC API user guidance, or user guidance)	A companion document – provided by the SPoC Solution Provider – with the optional SPoC libraries or SPoC API outlining the conditions and how the libraries or SPoC API can be used to interface the SPoC Solution. See Appendix D of the *SPoC Program Guide* and the *SPoC Standard* for additional information.
SPoC Vendor (or Vendor)	Any of the following: SPoC Solution Provider, PIN CVM Application and supporting Monitoring/Attestation System vendor, or Back-end Monitoring Environment provider.
Third-Party Service Provider	An entity that acts on behalf of a Solution Provider to provide a service or function that is incorporated into or utilized by the applicable Solution. A Third-Party Service Provider must have its services reviewed during the course of each of its Solution-Provider customers' SPoC Solution Evaluations.
Validated SPoC Solution	A SPoC Solution that has been assessed by a SPoC Lab to be in scope for the SPoC Program and to have met all of the SPoC Security Requirements and then Accepted by PCI SSC, so long as such Acceptance has not been revoked, suspended, withdrawn, or terminated.

Term	Definition / Source / Document Reference
Vendor Release Agreement (or VRA)	The then-current and applicable form of release agreement that PCI SSC: • Requires to be executed by SPoC Solution Providers, Monitoring/Attestation System or Back-end Monitoring Environment Providers and/or PIN CVM Application Vendors (as applicable) in connection with the SPoC Program, and • Makes available on the Website.
Website	The then-current PCI SSC Website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org.