Security Standards Council®

Payment Card Industry (PCI)
Contactless Payments on COTS (CPoC™)

Program Guide

Version 1.0

December 2019

Document Changes

Date	Version	Description
December 2019	1.0	Initial Release of the Contactless Payments on COTS (CPoC™) Program Guide

Table of Contents

1 Introduction

This Program Guide provides an overview of the PCI SSC Contactless Payments on Commercial Off-the-Shelf (COTS) (CPoC™) program operated and managed by PCI Security Standards Council, LLC, and should be read with the documents referenced in Section 1.2, *Related* Publications. This document applies primarily to PCI-recognized CPoC Laboratories (CPoC Labs) and Vendors developing and seeking validation of their CPoC Solutions. Capitalized terms, used but not otherwise defined in this document, are defined in or pursuant to *Appendix F* of this Program Guide.

This Program Guide describes the following:

- *CPoC Solution Overview* (Section 1.1)
- *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)
- *Quality Management Program* (Section 6.3)

1.1 CPoC Solution Overview

Each of the following elements of a CPoC Solution (or Solution) requires evaluation and validation for use within the Solution. Additionally, the CPoC Solution itself must be evaluated, and successfully validated and submitted to PCI SSC by a CPoC Lab, prior to Acceptance and listing by PCI SSC.

- **CPoC Application:** Evaluated by a CPoC Lab per the *CPoC Standard* as part of the lab's CPoC Solution Evaluation. CPoC Applications are listed only as part of the CPoC Solutions in which they have been validated for use under the CPoC Program and are not listed separately on the Website.
  - **CPoC Application Programming Interface (API):** An optional software component developed and provided by the Solution provider to allow third-party developers to interface with the CPoC Solution. APIs must be Evaluated by a CPoC Lab as part of the CPoC Solution Evaluation. CPoC APIs are listed only as part of the CPoC Solution in which they have been validated for use under the CPoC Program and are not listed separately on the Website.

- **Monitoring/Attestation System:** Evaluated by a CPoC Lab per the *CPoC Standard* as part of their overall CPoC Solution Evaluation. Monitoring/Attestation Systems are listed only as part of the CPoC Solutions in which they have been validated for use under the CPoC Program and are not listed separately on the Website.

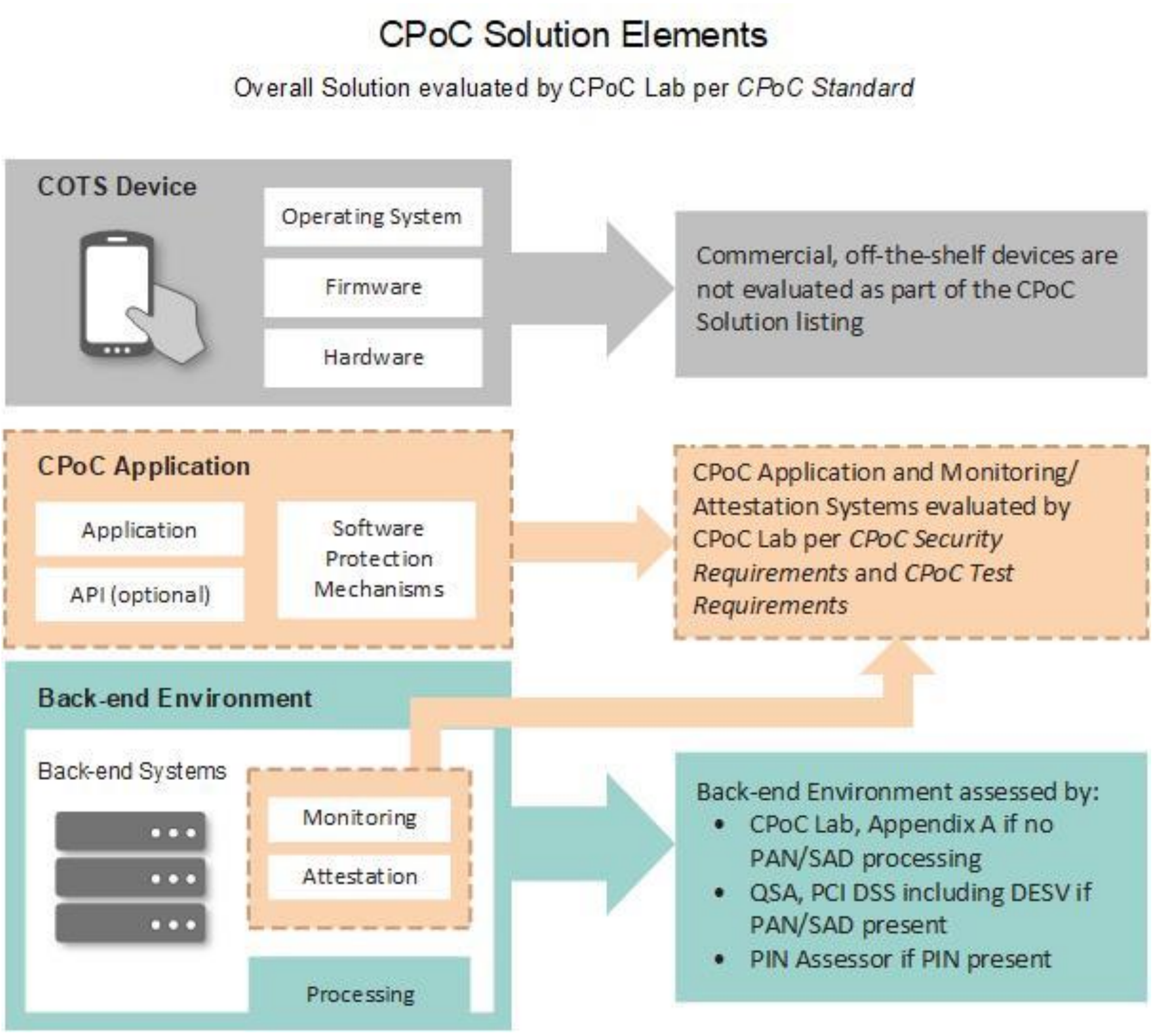
- **Back-end Monitoring Environment:** The environment in which the Monitoring/Attestation System resides and operates must undergo an onsite assessment by a CPoC Lab for compliance with the *CPoC Standard*, Appendix A "Monitoring Environment Basic Protections."

  Note: *If the Primary Account Number (PAN) or the 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 against the* PCI DSS, *including* PCI DSS *Appendix A3, "Designated Entities Supplemental Validation (DESV)."*

  Back-end Monitoring Environments are not listed on the Website.

Figure 1 illustrates each element of the CPoC Solution and the CPoC Program stakeholder that validates each respective element. For additional details, see the "Overview" and "Contactless Payments on COTS Devices" sections in the *CPoC Standard*.

Figure 1: CPoC Solution Elements


CPoC Solution Elements
Overall Solution evaluated by CPoC Lab per *CPoC Standard*
COTS Device
Operating System
Firmware
Hardware
Commercial, off-the-shelf devices are not evaluated as part of the CPoC Solution listing
CPoC Application
Application
API (optional)
Software Protection Mechanisms
CPoC Application and Monitoring/ Attestation Systems evaluated by CPoC Lab per *CPoC Security Requirements* and *CPoC Test Requirements*
Back-end Environment
Back-end Systems
Monitoring
Attestation
Processing
Back-end Environment assessed by:
• CPoC Lab, Appendix A if no PAN/SAD processing
• QSA, PCI DSS including DESV if PAN/SAD present
• PIN Assessor if PIN present

1.2 Related Publications

Use this Program Guide in conjunction with the latest versions of (or successor documents to) the following PCI SSC publications, which are available on the Website:

Table 1: Related Publications

Document Name	Description
Payment Card Industry (PCI) Contactless Payments on COTS Security and Test Requirements (*CPoC™ Security and Test Requirements*, or *CPoC Standard*)	The *CPoC Security and Test Requirements* (*CPoC Standard*) defines the specific technical security requirements and specific testing and evaluation procedures with which to evaluate the Solution, including the CPoC Application and the supporting Monitoring/Attestation System and Back-end Monitoring Environment.
CPoC™ Solution Attestation of Validation (AOV)	The *AOV* is a form for CPoC Labs to attest to the results of a CPoC Solution Evaluation, as documented in the *CPoC Solution Attestation of Validation*.
CPoC™ Evaluation Report template	The *Evaluation Report* template is a form for CPoC Labs to document the results of a CPoC Solution Evaluation.
Vendor Release Agreement (VRA)	The *VRA* establishes the terms and conditions under which validated Solutions are Accepted and listed by PCI SSC.

In addition to the documents listed in Table 1, see the following documents 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* (PCI Glossary)

1.3 Updates to Documents and Security Requirements

This *Program Guide* may be modified as necessary to align with updates or changes to the CPoC Program. Additionally, PCI SSC provides interim updates to the PCI community through a variety of means, including required Assessor or CPoC Lab training, e-mail bulletins and newsletters, frequently asked questions and other communication methods.

Technical FAQs are updated on a regular basis to add clarification to CPoC Program requirements and may also address new security threats. Generally, technical FAQs are 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 CPoC Program stakeholder groups. For details on evaluation, validation and listing of CPoC Solutions, see the following sections:

- Section 3, *Preparation for the Evaluation*
- Section 4, *Evaluation and Reporting Processes*
- Section 5, *Maintaining a Validated Solution Listing*

2.1 CPoC Vendors

Each vendor or provider of a candidate CPoC Solution, CPoC Application, Monitoring/Attestation System or Back-end Monitoring Environment under the CPoC Program, must provide access to the applicable CPoC Solutions or CPoC Elements and supporting documentation to its CPoC Labs for validation. The vendor or provider must also authorize its CPoC Labs to submit resulting reports and related information to PCI SSC.

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

2.1.1 CPoC Solution Providers

CPoC Solution Providers (for example, processors, acquirers or payment gateways) have overall responsibility for the design and implementation of specific Solutions. This includes ensuring that their Solutions satisfy all applicable CPoC security requirements, managing Solutions for their customers and/or managing corresponding responsibilities.

2.1.2 CPoC Application Vendors

Note: *The CPoC Application must be validated along with its supporting Monitoring/ Attestation System as part of the Solution in which it is used.*

Each software application Vendor that develops a CPoC Application must have that application evaluated for secure operation with the CPoC Solution in which it is used. The Vendor must provide the CPoC Lab with access to all corresponding unobfuscated source code and documentation that describes the secure installation and administration of such applications intended to work with the CPoC Application.

The Vendor (Solution Provider) submits a CPoC Application for evaluation, with its supporting Monitoring/Attestation System, to an independent CPoC Lab. Per the *CPoC Standard*, CPoC 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 (Monitoring/Attestation Systems) for a CPoC Application that is evaluated for use in a Solution. Monitoring/Attestation System Vendors must have their Monitoring/Attestation System evaluated and validated for compliance per the *CPoC Standard* with each CPoC Application that it supports.

The Solution provider submits a Monitoring/Attestation System for evaluation to an independent CPoC Lab. Per the *CPoC 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 validated Solution, Back-end Monitoring Environments must be evaluated onsite and validated by a CPoC Lab in accordance with *CPoC Standard*, Appendix A, “Monitoring Environment Basic Protections,” to ensure requirements are in place to protect systems and data in this environment.

If the Monitoring/Attestation System resides in a Back-end Monitoring Environment provider’s cardholder data environment (CDE), each Monitoring/Attestation System must also be validated by a QSA Company to *PCI DSS*, including *PCI DSS* Appendix A3, “Designated Entities Supplemental Validation (DESV).”

If PAN or SAD is not present in the Back-end Monitoring Environment, and it is not part of the Back-end Monitoring Environment provider’s existing CDE, a CPoC Lab must perform an onsite assessment and validate that the environment complies with the logical and physical security requirements defined in *CPoC Standard* Appendix A, “Monitoring Environment Basic Protections.”

> ***Note:*** *If the CPoC Solution Provider cannot meet DESV requirements at the point of an initial CPoC Solution validation, the Solution Provider must provide the CPoC Lab an action plan demonstrating that work is in progress for requirements to be met by the first annual checkpoint. The action plan will be reviewed by the CPoC 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 CPoC Solution.*

2.1.5 Third-Party Service Providers

Third-party service providers (such as key-injection facilities) are considered Third-Party Service Providers with respect to the CPoC Element or CPoC Solution for which they provide services, and their services are evaluated/assessed as part of each CPoC Element and/or CPoC Solution. A Third-Party Service Provider must have its third-party services reviewed during each CPoC Solution Evaluation in which its service is used.

Third-Party Service Providers are not eligible for listing in regard to the CPoC Program.

2.2 Entities Involved in CPoC Evaluations

The following entities are involved in CPoC Evaluations:

- PCI-recognized CPoC Laboratories (CPoC Labs)
- Participating Payment Brands
- PCI Security Standards Council (PCI SSC)

2.2.1 PCI-recognized CPoC Laboratories (CPoC Labs)

PCI-recognized CPoC Laboratories (CPoC Labs) are qualified by PCI SSC to perform Evaluations of Solutions for listing on the List of Validated CPoC Solutions. CPoC Labs are also qualified by PCI SSC to separately evaluate CPoC Applications and Monitoring/ Attestation Systems to be used in Solutions, as well as performing Back-end Monitoring Environment assessments (see *CPoC Standard*, Appendix A “Monitoring Environment Basic Protections”). For the purposes of the CPoC Program, CPoC Labs are responsible for:

- Evaluating CPoC Applications, Monitoring/Attestation Systems, Back-end Monitoring Environments and overall Solutions in accordance with the *CPoC Standard*
- Providing evidence to validate how the Solution meets the *CPoC Standard*
- Documenting each such Evaluation in an *Evaluation Report* using the applicable reporting templates
- Providing adequate documentation within the *Evaluation Report* to demonstrate the Solution’s compliance with the *CPoC Standard*
- Submitting the applicable *Evaluation Report* and/or any change submission documentation to PCI SSC, with the applicable *CPoC Solution Attestation of Validation* (AOV) signed by both the CPoC Lab and Vendor
- Maintaining an internal quality assurance process for their CPoC Solution Evaluation efforts

Entities interested in becoming a CPoC Lab should contact PCI SSC.

2.2.2 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 dates for compliance)
- Establishing penalties and fees
- Establishing requirements and who must validate
- Responding to cardholder data compromises

2.2.3 PCI Security Standards Council (PCI SSC)

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

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

Note: *PCI SSC does not evaluate or validate CPoC Solutions for CPoC compliance; evaluation and validation are the roles of the CPoC Labs. The listing of a Solution on the List of Validated CPoC Solutions signifies only that the applicable CPoC Lab has determined that the Solution complies with the CPoC Standard, that the CPoC Lab has submitted a* corresponding *Evaluation Report* to *PCI SSC and that the report, as submitted to PCI SSC, has satisfied all PCI SSC requirements as of the time of PCI SSC's review.*

3 Preparation for the Evaluation

The *CPoC Standard* is a cross-functional PCI SSC standard that includes specific requirements validated through the CPoC Program and, where applicable, the PCI DSS Assessment/QSA Program. The *CPoC Standard* also contains requirements for Solutions and CPoC Solution Elements (CPoC Applications, Monitoring/Attestation Systems and Back-end Monitoring Environments).

Note: *CPoC Vendors, CPoC Labs and Assessors are expected to be acutely familiar with each module within the CPoC Standard before beginning an Evaluation*.

3.1 Considerations for Elements Used in CPoC Solutions

Table 2 describes the requirements and eligibility for the various elements used in CPoC Solutions, including references to the relevant documents and sections:

Table 2: Elements Used in CPoC Solutions

Element	Program Guidance
CPoC Application (or CPoC API, if present)	A CPoC Lab must validate CPoC Applications against: • *CPoC Standard* Appendix D, "Software Security Requirements" A CPoC Application (and its supporting Monitoring/Attestation System) may be used in multiple Solutions, but it is considered a CPoC Element of only the specific Solutions for which it has been tested and validated in accordance with CPoC Program requirements.
Monitoring/Attestation System	A CPoC Lab must validate Monitoring/Attestation Systems against: • *CPoC Standard*, including Module 3, "Back-end Systems – Monitoring/Attestation" • *CPoC Standard* Module 4, "Solution Integration Requirements" A Monitoring/Attestation System (and the CPoC Application it supports) may be used in multiple Solutions, but it is considered a CPoC Element of only the specific Solutions for which it has been tested and validated in accordance with CPoC Program requirements.
Back-end Monitoring Environment	The Back-end Monitoring Environment must be validated by CPoC Lab personnel per all requirements of the *CPoC Standard* Appendix A, "Monitoring Environment Basic Protections." The CPoC Lab personnel must be physically onsite for each assessment, though the duration of the on-site visit will vary. If PAN or SAD is present anywhere in the Back-end Monitoring Environment, then a QSA must validate the environment for compliance with *PCI DSS* including *PCI DSS* Appendix A3, "Designated Entities Supplemental Validation (DESV)." In such cases, the Vendor's PCI DSS Attestation of Compliance (AOC) would be provided to the CPoC Lab during the CPoC Solution Evaluation as evidence of a compliant Back-end Monitoring Environment.
Back-end Processing Environment *(if separated from the Back-end Monitoring Environment)*	The Back-end Processing Environment where cardholder data is decrypted and securely processed must be validated per the *CPoC Standard* Module 4, "Back-end Systems – Processing" and must undergo PCI DSS validation. The Vendor's PCI DSS Attestation of Compliance (AOC) is provided to the CPoC Lab during the CPoC Solution Evaluation as evidence of a compliant Back-end Processing Environment.

3.2 Prior to the Evaluation

Note: *The Solution development and test process is defined in the CPoC Standard. These documents include guidance for implementing requirements, testing and validating compliance with each requirement.*

Before starting a CPoC Solution Evaluation, all involved parties should do the following to prepare:

- Review the *CPoC Standard* and all related documentation located on the Website.
- Determine the Solution's readiness to comply with the *CPoC Standard*:
  - Perform a gap analysis between security function and the *CPoC Standard.*
  - Correct any gaps
  - If desired, the CPoC Lab may perform a pre-evaluation or gap analysis of a candidate CPoC Element or candidate CPoC Solution. If the CPoC Lab notes deficiencies that would prevent compliance, the CPoC Lab may provide a list of issues to the Vendor to be addressed before the formal Evaluation process begins.
- CPoC Solution Providers are responsible for ensuring that the various Solution elements used as parts of their Solutions are each compliant with all applicable *CPoC security requirements*, and that the appropriate agreements are in place with the providers and vendors of such elements to ensure proper information disclosures (if required) under the *Vendor Release Agreement*.

3.3 Required Documentation

When submitting a Solution for initial Evaluation and listing, the Vendor must provide the CPoC Lab with the documentation described in the *CPoC Standard.*

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

3.4 Evaluation and Review Timeframe Considerations

The time needed for the CPoC Lab to complete its work can vary widely depending on factors such as:

- Candidate Solution or Element initial level of compliance with the CPoC Program requirements—more corrections mean a longer validation.

- Prompt payment of the fees to PCI SSC. PCI SSC will not start the review process until the applicable fees are paid.
- Quality of the CPoC Lab's submission to PCI SSC. For example:
  - Incomplete submissions or error, missing, incomplete or unsigned documents will delay the review process.
  - Multiple review/correction iterations between PCI SSC and the CPoC Lab will delay the review process.

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

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

3.5 Technical Support throughout Testing

A Vendor technical-resource representative should be available to assist with any questions that 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 CPoC Lab.

3.6 Vendor Release Agreement (VRA)

Before PCI SSC will review any Solution (or candidate Solution) submission for listing on the Website, the Vendor must provide a signed copy of the then-current *Vendor Release Agreement* (VRA) to the CPoC Lab. The current version of the *VRA* is available on the Website. In addition, at the beginning of each CPoC Solution Evaluation process, the Vendor must provide access to the Solution and other documents and materials.

The *VRA* addresses the following and other topics:

- Confidentiality issues
- Vendor's agreement with the CPoC Program requirements, policies and procedures

- Permission for the Vendor's CPoC Lab to release *Evaluation Reports*, *AOVs* and related materials to PCI SSC for review
- Vendor's agreement to adopt and comply with industry-standard Vulnerability Handling Policies

For PCI SSC to review an *Evaluation Report*, the CPoC Lab must provide PCI SSC with the Vendor's signed copy of the then-current *VRA* and the initial *Evaluation Report* (and *AOV* and related materials, as applicable) that was submitted to PCI SSC in connection with that Evaluation.

While an executed copy of the then-current *VRA* is on file with PCI SSC for the relevant Vendor, the CPoC Lab is not required to resubmit the same *VRA* with subsequent *Evaluation Reports* (or *AOV* or related materials, as applicable) for the same Vendor.

3.7 The Portal

To list a Solution on the Website, the CPoC Lab, (on behalf of the Vendor) must submit all Solution-validation documents to PCI SSC through the secure CPoC portal on the PCI SSC Website (Portal). PCI SSC staff screens submissions in the Portal to ensure that all required documentation has been included, and that the basic submission requirements have been satisfied.

PCI SSC also uses the Portal to track communications for each submission.

3.8 CPoC Program Acceptance Fees

To list a Solution on the Website, the Vendor must pay an Acceptance Fee to PCI SSC. For each new Solution submission, PCI SSC sends an invoice for the Acceptance Fee to the Vendor. PCI SSC must receive payment before the submission will be reviewed, Accepted and added to the List of Validated CPoC Solutions. Upon Acceptance, PCI SSC signs and returns a copy of the corresponding *AOV* to both the Vendor and the CPoC Lab.

Note: *The Vendor pays all Evaluation fees directly to the CPoC Lab. The CPoC Lab negotiates these fees with its customers. PCI SSC bills the Vendor for the Acceptance Fee, and the Vendor pays this fee directly to PCI SSC.*

There are no recurring annual PCI SSC fees associated with the Acceptance of a CPoC Solution. There are, however, PCI SSC fees associated with Vendor delays in annual Solution revalidation. For more information, see the Website.

All CPoC 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 is a high-level overview of the CPoC Solution Evaluation process.

1. The CPoC Vendor (Vendor) contracts with a CPoC Lab to evaluate the Solution and negotiates the cost and any associated confidentiality and non-disclosure agreements with the CPoC Lab.
2. The Vendor provides the CPoC Lab with access to all CPoC Solution Elements to be evaluated, as well as the signed *VRA*, associated manuals and other required documentation. The CPoC Lab may also require access to the Back-end Monitoring Environment to validate the Monitoring/Attestation System.

   When the Monitoring/Attestation System resides in a Back-end Monitoring Environment provider's CDE, each of these must adhere to *PCI DSS*, including *PCI DSS* Appendix A3, "Designated Entities Supplemental Validation (DESV)."

   If PAN or SAD is *not* present in the Monitoring/Attestation System's environment; that is, the Monitoring/Attestation System is not part of the Back-end Monitoring Environment provider's existing CDE, the environment must comply with the logical and physical security requirements defined in the *CPoC Standard* Appendix A, "Monitoring Environment Basic Protections."
3. The CPoC Lab evaluates the CPoC Solution, including evaluation of security functions and features. The Evaluation determines whether the candidate Solution and its Elements comply are validated in accordance with the *CPoC Standard*.
4. The CPoC Lab completes the *Evaluation Report*.
5. If the CPoC Lab determines that the Solution complies with the applicable CPoC security requirements, the CPoC Lab submits the corresponding *Evaluation Report*, the *AOV* (for each Solution), the Vendor's signed *VRA* and any other requested documentation to PCI SSC in accordance with applicable PCI SSC templates, guidance and instructions.
6. If required, the Vendor performs remedial activities to address security objectives or requirements that are not in place, or security controls for which there was insufficient evidence. The CPoC Lab then performs follow-up testing and provides PCI SSC with an updated *Evaluation Report*.
7. PCI SSC issues an invoice to the Vendor for the Acceptance Fee. After the Vendor pays the invoice, PCI SSC reviews the *Evaluation Report* to confirm that it meets the CPoC Program requirements and, if confirmed, PCI SSC notifies the CPoC Lab and Vendor that the Solution has successfully completed the process.
8. PCI SSC countersigns the *AOV* and sends a copy to the Vendor and the CPoC Lab.
9. PCI SSC adds the Solution to the List of Validated CPoC Solutions on the Website.

***Note:** To be published on the List of Validated CPoC Solutions, a Solution must, at a minimum, contain one of each successfully validated CPoC Application and Monitoring/Attestation System and be implemented in a compliant Back-end Monitoring Environment.*

4.1 Required Vendor Materials

The Solution provider must provide sufficient evidence to enable a CPoC Lab to validate the Solution against the *CPoC 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. 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 functions, including bespoke or custom functions developed by third parties and any APIs provided as part of the Solution

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 Vendor or CPoC Solution/CPoC Element cannot meet a specific requirement as stated, the Vendor must clearly explain why the requirement cannot be met as stated. The Vendor 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 are employed to provide equivalent or greater assurance to that provided by the methods described in the requirement. Vendors should work with their CPoC Lab to determine the evidence required to satisfy a specific security objective or associated requirement. The CPoC 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

Solutions for different major operating system versions and major versions of the *CPoC Standard* represent different Solutions as far as the *CPoC Standard* is concerned. Each update to a Solution to support a new or different major COTS device operating system version, or a new major version of the *CPoC Standard*, must undergo a new, complete Evaluation of the entire CPoC Solution.

4.3 Integrating CPoC Elements

CPoC Solutions that leverage security services from elements defined within the CPoC architecture that 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 each Evaluation. CPoC Vendors 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 CPoC Lab. Moreover, as part of the Evaluation, the CPoC Lab must evaluate the interaction between the Solution and such security services.

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

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

The illustrations and descriptions on the following pages show the CPoC Program processes in more detail:

- Figure 2 shows the CPoC Solution Evaluation and PCI SSC listing process.
- Figure 3 shows the CPoC Solution submission and PCI SSC review process.

Figure 2: CPoC Solution Evaluation for PCI SSC Listing

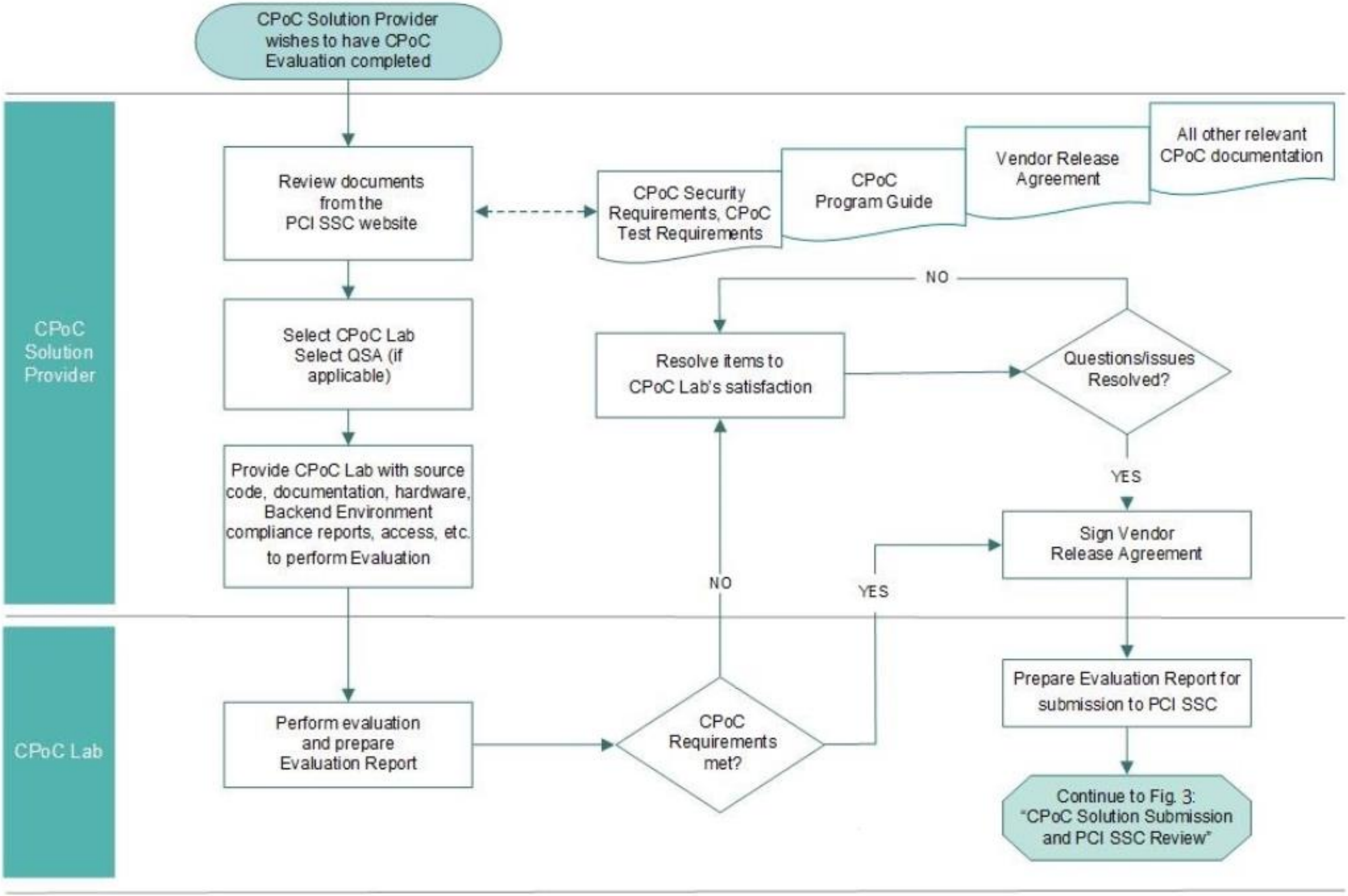
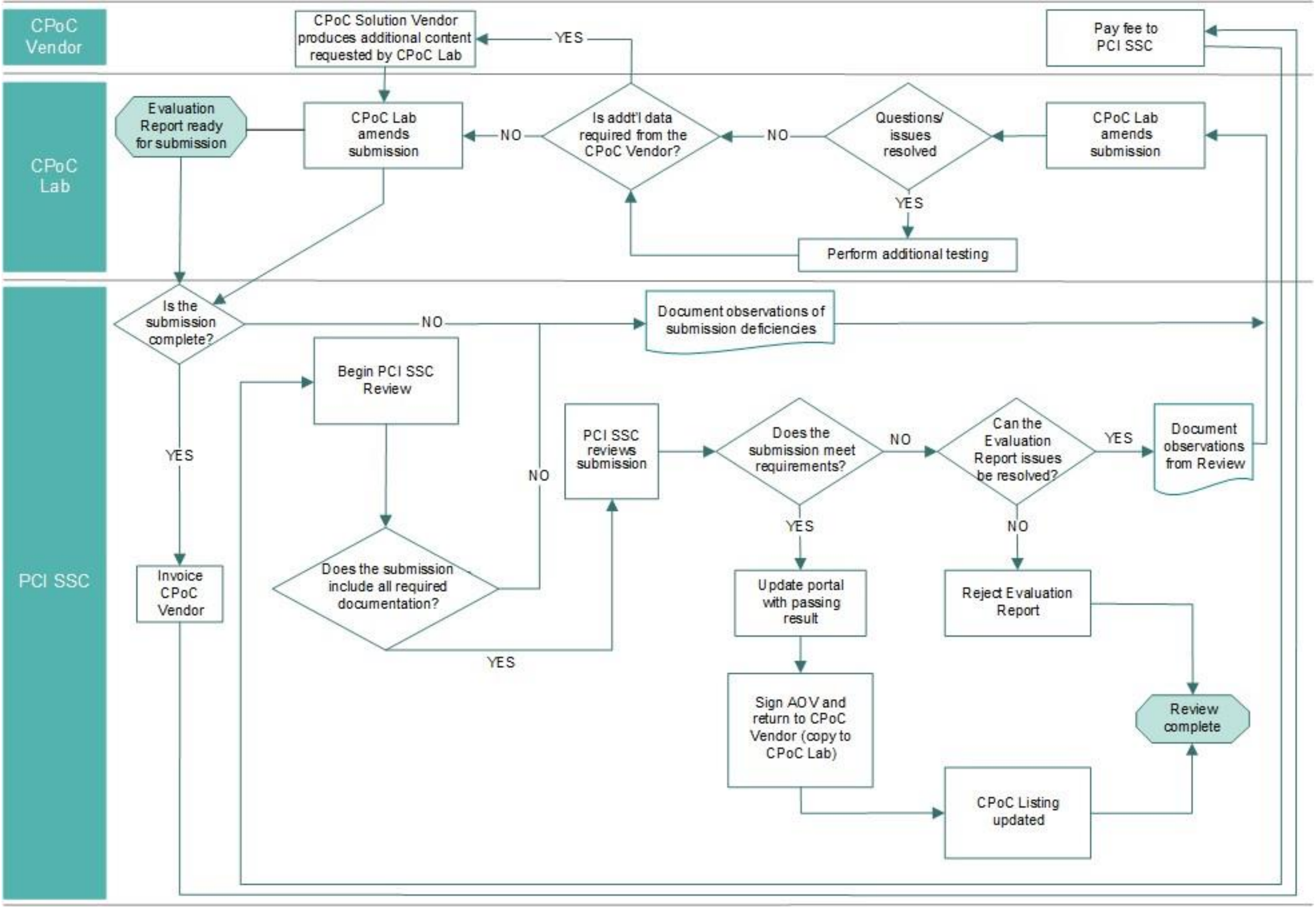

CPoC Solution Provider wishes to have CPoC Evaluation completed
CPoC Solution Provider
CPoC Lab
Review documents from the PCI SSC website
CPoC Security Requirements, CPoC Test Requirements
CPoC Program Guide
Vendor Release Agreement
All other relevant CPoC documentation
Select CPoC Lab
Select QSA (if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

Figure 3: CPoC Solution Submission and PCI SSC Review


CPoC Vendor
CPoC Lab
PCI SSC
CPoC Solution Vendor produces additional content requested by CPoC Lab
YES
Pay fee to PCI SSC
Evaluation Report ready for submission
CPoC Lab amends submission
NO
Is addt'l data required from the CPoC Vendor?
NO
Questions/ issues resolved
CPoC Lab amends submission
YES
Perform additional testing
Is the submission complete?
NO
Document observations of submission deficiencies
Begin PCI SSC Review
YES
NO
PCI SSC reviews submission
Does the submission meet requirements?
NO
Can the Evaluation Report issues be resolved?
YES
Document observations from Review
YES
NO
Invoice CPoC Vendor
Does the submission include all required documentation?
Update portal with passing result
Reject Evaluation Report
YES
Sign AOV and return to CPoC Vendor (copy to CPoC Lab)
Review complete
CPoC Listing updated

5 Maintaining a Validated Solution Listing

This section describes requirements for reevaluating and maintaining validated Solutions.

In each three-year cycle, annual "checkpoints" are required on or before each yearly anniversary of the original date of Acceptance, referred to as the *Annual Checkpoint Due* date (shown on the List of Validated CPoC Solutions).

Each three-year anniversary from the date of Acceptance is referred to as a *Reevaluation Date* (shown on the List of Validated CPoC Solutions). A new full Evaluation is required on or before the Reevaluation Date (the Solution's expiry date).

5.1 Annual Checkpoints

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

Vendors must perform checkpoints at 12- and 24-month intervals from the date of Acceptance or the date of last successfully completed full Evaluation (whichever is most recent), including submission of an updated *CPoC Solution AOV* to PCI SSC at each annual checkpoint. Each checkpoint submission must be made by a CPoC Lab; CPoC Labs must review all changes to the CPoC Solution 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 CPoC Lab must also perform live testing to ensure that the Solution remains compliant with all applicable CPoC security requirements. Live testing means full testing on active production-level COTS devices, the CPoC Application and its Monitoring/Attestation System[1].

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

Note: *Vendors should submit annual checkpoint documentation and attestation to the CPoC Lab that performed the last full CPoC Solution Evaluation. Changing CPoC Labs requires a full CPoC Solution Evaluation.*

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

[1] Including any optional APIs offered by the Solution provider to interface the CPoC Solution.

- Changes have been applied in a way that is consistent with the *CPoC Standard.*
- The Solution continues to meet all applicable CPoC security requirements.
- The Vendor is capable of and demonstrably migrating merchants from unsupported COTS platforms.
- PCI SSC has been advised of any change that requires an update to the Listing on the Website, in accordance with this *Program Guide*.
- Changes to the documents described in the *CPoC Standard* are provided to the CPoC Lab for review annually (12-month and 24-month checkpoints).
- The operational quality of the Monitoring/Attestation System has been assessed per the *CPoC Standard,* including Module 3.

The Vendor must consider the impact of external threats and whether updates to the Solution are necessary to address changes to these threats. The CPoC Lab submits the updated *AOV*, redlined *CPoC Solution Evaluation Report* and any applicable documentation to the PCI SSC CPoC Program Manager using the Portal. An updated *AOV* and redlined *Evaluation Report* must be submitted to PCI SSC ahead of the annual checkpoint date. PCI SSC has calendar 30 days to review and accept the submittal.

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

If PCI SSC does not receive the submittal before the annual checkpoint date, the Listing will be subject to early administrative expiry as follows:

- 14 calendar days following the annual checkpoint date, the corresponding Listing will be updated to show its annual checkpoint date in **Orange** for a period of 90 calendar days past its 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 will be updated to show its annual checkpoint date in **Red**. This indicates that a full Evaluation (including applicable fee) is required before returning 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 Vendor and CPoC Lab.

3. Update the annual checkpoint date on the Website.

5.2 Changes to CPoC Solution Listings

Vendors may update listed CPoC Solutions for various reasons. Changes do not have any impact on the Listed Solution's Reevaluation Date (Solution expiry dates or annual checkpoint dates). Table 3 describes the change types for Listed Solutions.

***Note:** Any change to the CPoC Solution that requires the code to be recompiled (in order to accommodate the change) requires an update to the Solution's Listing.*

Table 3: Changes to Listed Solutions

Change Type	Description
Administrative	Changes made to a listed Solution that do not impact compliance with any of the CPoC security requirements, and where the List of Validated CPoC Solutions is updated to reflect the change, for example, corporate identity changes. For details, see Section 5.2.1, *Administrative Changes for CPoC Solution Listings*.
No Impact Change	Changes that do not impact security functions or compliance with any of the CPoC security requirements, such as maintenance patches or routine key rotation. No Impact Changes are not reported in detail but are addressed by the Vendor during the annual checkpoint. No Impact Changes are *not* reflected on the List of Validated CPoC Solutions.
Delta Change	Changes that are non-high impact where the CPoC Lab determines that the change is a low security risk or has a low impact on compliance with the CPoC Standard. Delta Changes can be assessed separately; that is, a full Evaluation is not required to validate the change. For details, see Section 5.2.22, *Delta Changes*.
High-impact Change	Changes where the CPoC Lab determines that the change is a high security risk or has a significant impact on the overall CPoC 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* for details). For details, see Section 5.2.33, *High-impact Changes*.

5.2.1 Administrative Changes for CPoC Solution Listings

Administrative Changes are limited to updates where no changes to a listed CPoC Solution have occurred, but the Vendor 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 Vendor prepares a change analysis using the *Change Impact* template (*Appendix C*) and submits it to the CPoC Lab for review. At a minimum, the change analysis must contain the following information:

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

The Vendor should submit a change analysis to the same CPoC Lab that performed the original CPoC Solution Evaluation. Changing CPoC Labs requires a full Evaluation of the Solution. If the CPoC Lab agrees that the change is eligible as an Administrative Change

If the CPoC Lab does not agree that the change is eligible as an Administrative Change, the CPoC Lab works with the Vendor to resolve the disagreement. If the CPoC Lab agrees that the change is an Administrative Change:

1. The CPoC Lab notifies the Vendor that the change qualifies as an Administrative Change.
2. The Vendor prepares the change documentation, signs the corresponding *AOV* (and new *VRA*, if applicable) and sends all applicable documentation (see Table 5) to the CPoC Lab.
3. The CPoC Lab completes the corresponding change documentation and signs its concurrence on the corresponding *AOV*.
4. The CPoC Lab forwards the *AOV* with the corresponding change documentation (and new *VRA* if applicable) to PCI SSC.
5. PCI SSC sends an invoice to the Vendor for the applicable change fee.
6. Upon payment of the invoice, PCI SSC reviews the submission.

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

1. Updates the List of Validated CPoC Solutions on the Website with the new information.
2. Signs and returns a copy of the corresponding *AOV* to the Vendor and the CPoC Lab. The Reevaluation Date of the updated Listing remains the same as that of the parent Listing.

Should there be quality issues associated with any aspect of the submission, PCI SSC will communicate them to the CPoC Lab. PCI SSC reserves the right to reject any submission if it determines that any corresponding change is not an Administrative Change.

5.2.2 Delta Changes

Delta Changes are changes made to a CPoC Solution or CPoC Element (for example, a CPoC Application and/or supporting Monitoring/Attestation System) and are limited to changes where the CPoC Lab appropriately determines that a partial evaluation (Delta Evaluation) can be performed, rather than a full Evaluation of the CPoC Solution. For example, changes to the CPoC Application that impact only the tamper-protection features may be eligible for a Delta Evaluation.

Because the number of possible changes and their impact cannot be determined in advance, the type of evaluation required must be considered on a per-case basis. Vendors should contact the CPoC Lab that performed the last full Solution Evaluation for guidance. The CPoC Lab makes its determination whether a Delta Evaluation or full Evaluation is required based on the scope of the changes and the impact on the following:

- Security
- CPoC-related functions of the CPoC Element
- *CPoC Standard*

For detailed information about the content of the change analysis, see Section 5.3, *Change Documentation*.

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

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

The Vendor should submit the change analysis to the same CPoC Lab that performed the previous full Evaluation. Changing CPoC Labs requires a full Evaluation of the CPoC Solution.

If the CPoC Lab does not agree that the change is eligible as a Delta Change, the CPoC Lab works with the Vendor to resolve the disagreement. If the CPoC Lab agrees that the change is a Delta Change:

1. The CPoC Lab notifies the Vendor that the change qualifies as a Delta Change.
2. The Vendor prepares the change documentation, signs the corresponding *AOV* (and new *VRA*, if applicable) and sends all applicable documentation (see Table 5) to the CPoC Lab.

3. The CPoC Lab evaluates the CPoC security requirements that are affected by the change and performs all applicable integration testing.
4. The CPoC Lab completes the corresponding change documentation and produces a red-lined *Evaluation Report* documenting that testing is complete per PCI SSC requirements.
5. The CPoC Lab signs its concurrence on the *AOV* and forwards it with the completed change documents, *VRA* (as applicable) and the red-lined *Evaluation Report* to PCI SSC.
6. PCI SSC sends an invoice to the Vendor for the applicable change fee.
7. Upon payment of the invoice, PCI SSC reviews the submission.

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

1. Updates the List of Validated CPoC Solutions on the Website with the new information.
2. Signs and returns a copy of the corresponding *AOV* to the Vendor and the CPoC Lab. The Reevaluation Date of the updated Listing remains the same as that of the parent Listing.

Should there be quality issues associated with any part of the submission, PCI SSC will communicate them to the CPoC Lab. PCI SSC reserves the right to reject any submission if it determines that any corresponding change is not a Delta Change.

5.2.3 High-impact Changes

High-impact Changes are changes made to a CPoC Solution or CPoC Element (for example, a CPoC Application and/or supporting Monitoring/Attestation System) where the CPoC Lab appropriately determines that the magnitude of the change is greater than what can be validated by a Delta Evaluation; therefore, a complete (full) Evaluation of the CPoC Solution is necessary. For example, a High-impact Change might impact multiple modules of the *CPoC 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 required must be considered on a per-case basis. Vendors should contact the CPoC Lab that performed the last full Solution Evaluation for guidance. The CPoC Lab makes a determination whether a full Evaluation is required, based on the scope of the changes and impact on the following:

- Security
- CPoC-related functions
- *CPoC Standard*

5.3 Change Documentation

Table 4 summarizes the change documentation.

Table 4: 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* • Current *VRA* [b]

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

[b] If applicable.

5.4 Acceptance and Change Fees

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

Prior to Acceptance, the Vendor must pay the applicable Acceptance Fee to PCI SSC. For any change affecting the validated CPoC 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 Vendor and the CPoC Lab and updates the List of Validated CPoC Solutions.

There is no PCI SSC fee for processing of annual checkpoints.

All CPoC Program fees are posted on the Website (see Fee Schedule). CPoC 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 Vendor of the pending expiration. There are two options available for the Vendor: a new Evaluation or expiry.

- **New Validation:** If the Vendor wants the Solution Listing to remain on the List of Validated CPoC Solutions, the Vendor must engage a CPoC Lab to perform a new full Evaluation *prior to the expiry date*. The CPoC Lab performs the Evaluation against the then-current version of the *CPoC Standard*, resulting in a new Acceptance. This Evaluation must follow the same process as a new CPoC 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, and in **Red** thereafter.

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

In the event of a Security Issue (as defined in the *VRA*) relating to a validated CPoC Solution, the *VRA* requires the Vendor to notify PCI SSC. Vendors must be aware of and adhere to their obligations under the *VRA*.

6 Reporting Considerations

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.*

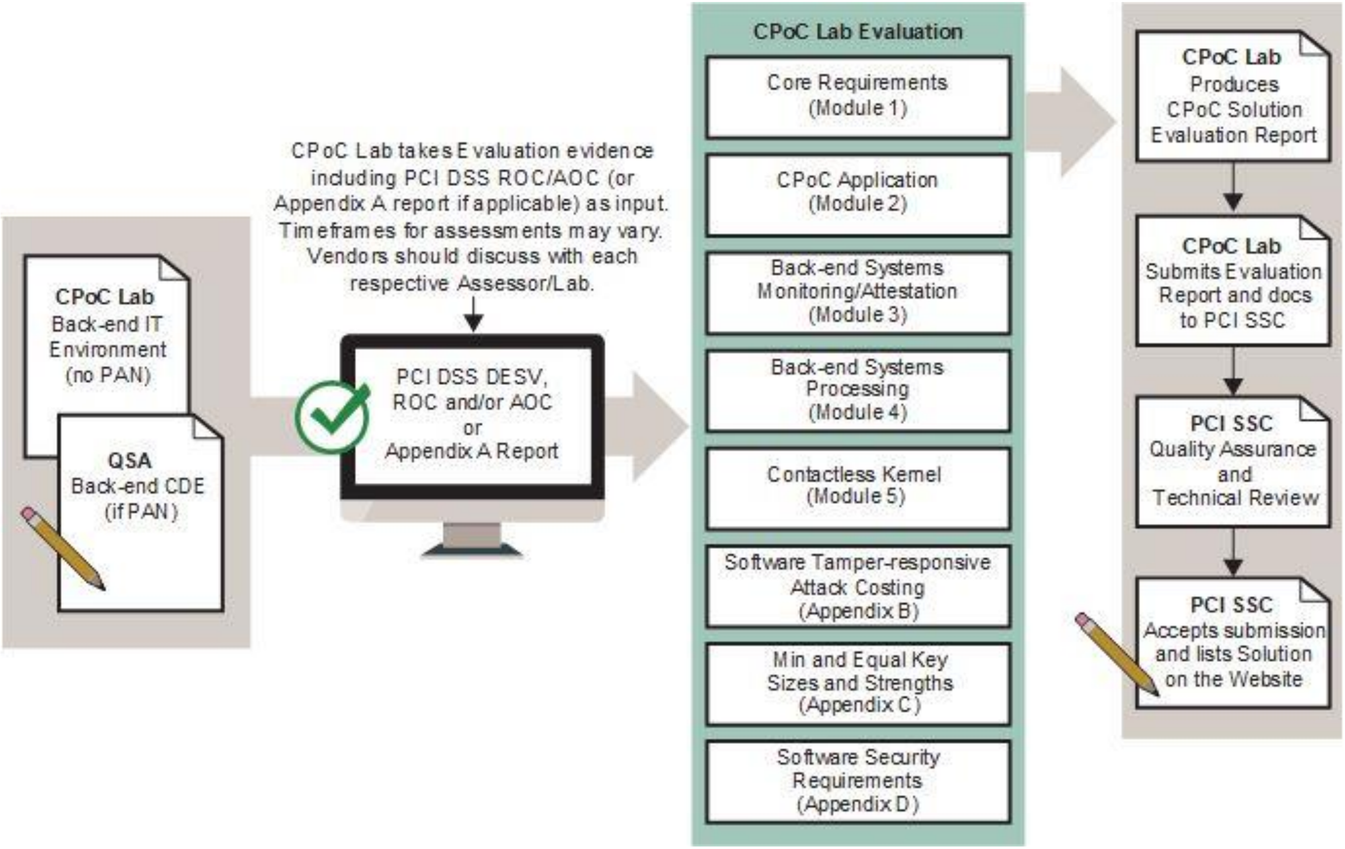
Upon receipt of the submission for a new CPoC Solution, PCI SSC identifies any technical issues or questions for resolution by the CPoC Lab, typically within two calendar weeks of receipt. Subsequent Lab responses and information will be reviewed, and the cycle will repeat until satisfactory responses 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 CPoC 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 revised countersigned AOV. Delta reports for a given Solution are prepared using the same major requirements that were used for the Evaluation of that Solution that resulted in its Acceptance.

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

Figure 4: CPoC Solution Submittal, Evaluation, Review and Acceptance Process


CPoC Lab
Back-end IT Environment (no PAN)
QSA
Back-end CDE (if PAN)
CPoC Lab takes Evaluation evidence including PCI DSS ROC/AOC (or Appendix A report if applicable) as input. Timeframes for assessments may vary. Vendors should discuss with each respective Assessor/Lab.
PCI DSS DESV, ROC and/or AOC or Appendix A Report
CPoC Lab Evaluation
Core Requirements (Module 1)
CPoC Application (Module 2)
Back-end Systems Monitoring/Attestation (Module 3)
Back-end Systems Processing (Module 4)
Contactless Kernel (Module 5)
Software Tamper-responsive Attack Costing (Appendix B)
Min and Equal Key Sizes and Strengths (Appendix C)
Software Security Requirements (Appendix D)
CPoC Lab Produces CPoC Solution Evaluation Report
CPoC 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

For CPoC Solutions to be listed on the Website, the CPoC Lab must submit all required CPoC validation process documents to PCI SSC through the Portal. PCI SSC screens Portal submissions 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. Incomplete or inconsistent submissions will 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 CPoC Lab submits must track cumulative changes.

6.3 Quality Management Programs

Assessors and CPoC Labs must meet all applicable quality assurance requirements set by PCI SSC.

6.3.1 Evaluation Report Submission Review

PCI SSC reviews each *Evaluation Report* submission after the Vendor pays the Acceptance Fee. PCI SSC performs an administrative review (pre-screening) to ensure that the submission 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 CPoC Program requirements, including but not limited to the *CPoC Program Guide*. If eligibility is in question, PCI SSC contacts the CPoC Lab for additional information. If the candidate Solution is ineligible for validation under the CPoC Program, the *Evaluation Report* is rejected, and the CPoC Lab will receive a letter of rejection with instructions for appeal.

If the candidate Solution is eligible for validation under the CPoC Program and the submission is complete, PCI SSC conducts a complete review of the *Evaluation Report* submission and supporting documentation provided or subsequently requested by PCI SSC. PCI SSC transmits any comments or feedback through the Portal, which the CPoC Lab is expected to address in a timely manner. PCI SSC's role is to ensure that the CPoC Lab's submission contains sufficient evidence that the CPoC Solution Evaluation was performed in accordance with CPoC Program requirements and quality standards.

Appendix A CPoC Program Acceptance

Acceptance of a given CPoC Solution or CPoC Element by PCI SSC applies only to the specific CPoC Solution or CPoC Element that has been validated by a CPoC Lab and subsequently Accepted by PCI SSC (each an Accepted CPoC Solution or Accepted CPoC Element). If any aspect of a CPoC Solution or CPoC Element is different from that which was validated by the CPoC Lab and Accepted by PCI SSC—even if the different CPoC Solution or CPoC 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 CPoC Vendor or other third party may refer to a CPoC Solution or CPoC 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 CPoC Vendor or its CPoC Solution or CPoC 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 CPoC Solution or CPoC 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 CPoC Vendor or the functionality, quality or performance of the CPoC Solution or CPoC 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 CPoC Solutions

Table 5: Elements for the List of Validated CPoC Solutions

<table>
<tr><th>Entry</th><th></th></tr>
<tr><td><b>Company</b></td><td>The CPoC Solution Provider for the validated Solution.</td></tr>
<tr><td><b>Solution Identifier</b></td><td>A subset of fields in the Listing below the <b>Company</b> entry used by PCI SSC to denote relevant information for each validated Solution, consisting of the following fields:
<table>
<tr><th>Field</th><th>Detail</th></tr>
<tr><td><b>Solution Name</b></td><td>Name supplied by the CPoC Solution Provider under which the Solution is sold.</td></tr>
<tr><td><b>Solution Version</b></td><td>Version of the CPoC Solution provided by the CPoC Solution Provider</td></tr>
<tr><td><b>Reference Number</b></td><td>A number assigned by PCI SSC when the validated Solution is posted to the Website. This number is unique per CPoC Solution Provider and CPoC Solution and remains the same for the life of the Listing.
An example reference number is 2019-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</td></tr>
</table>
</td></tr>
<tr><td><b>CPoC Version</b></td><td>The version of the CPoC standard used to evaluate and validate Solution compliance</td></tr>
<tr><td><b>Evaluation Lab</b></td><td>The name of the CPoC Lab that performed the Evaluation and validated that the Solution is compliant with all applicable CPoC security requirements.</td></tr>
<tr><td><b>Reevaluation Date</b></td><td>The date by which the Vendor must have the Solution fully re-evaluated and validated against the current <i>CPoC Standard</i> to maintain the Acceptance.
<b>Orange</b>- or <b>Red</b>-colored indicators next to this field signify that the Solution is overdue for submittal to PCI SSC.</td></tr>
<tr><td><b>Annual Checkpoint Due</b></td><td>The date that the Solution is due for its 12- and 24-month checkpoints by a CPoC Lab.
<b>Orange</b>- or <b>Red</b>-colored indicators by this field signify that the Solution is overdue for submittal to PCI SSC.</td></tr>
<tr><td><b>Supported CPoC Application</b></td><td>The name of the CPoC Application (and/or optional API) that is installed and executed on the merchant COTS device for the purposes of accepting and processing account data associated with a contactless transaction.</td></tr>
</table>

Appendix C Change Impact Template

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

The Solution Provider and CPoC Lab must complete each applicable section of this document and all other required documents based on the type of change (see tables in Section 5.2). The CPoC Lab must submit this CPoC *Change Impact* with supporting documentation to PCI SSC for review.

Part 1. CPoC Solution Listing Details, Contact Information and Change Type

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

Vendor Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	

CPoC 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 Vendor (Solution Provider) Company Name		Revised Vendor Company Name *(if applicable)*	
Current CPoC Solution or CPoC Element Name		Revised CPoC Solution or CPoC Element 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(s) applicable to this submission and provide the following information.

Changes that impact compliance with the *CPoC Standard* must be reflected in the submitted red-lined *Evaluation Report*. Use additional rows or add pages if needed.

Delta Change – Change Summary			
Change #	Detailed description of the change	Description of the purpose of the change	Description of how CPoC security is impacted
Description of how this change is reflected in the Vendor’s versioning methodology, if applicable, including how this version number indicates the type of change			
Additional details, as applicable:			

Generate a red-lined *CPoC Solution Evaluation Report* for the changes (as applicable).

Appendix D CPoC Vendor-provided Libraries or APIs

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

- The CPoC Solution Provider is responsible for the development and validation of the libraries or API and a companion document ("user guidance") outlining the conditions and how the libraries or API can be used to interface the CPoC 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 CPoC Solution Provider is responsible for all terms and conditions in the user guidance and must submit the user guidance to the CPoC Lab as part of each CPoC Solution Evaluation (or applicable change submittal) for which libraries or an API is provided.
    - The CPoC Solution Provider must make the user guidance available to all third parties that interface the CPoC Solution via the provided libraries or API.
- The CPoC Lab must assess the libraries or API (and any associated software) and the companion user guidance as part of each applicable CPoC Solution Evaluation, or applicable change submittal.
    - The CPoC Lab must validate that usage of the libraries or API (e.g., integration of a user interface or business logic with a CPoC Solution) can be done without violating or negatively impacting any of the CPoC security requirements.
    - The API will be listed under the CPoC Solution Details page in the website listing as a "Supported CPoC Application."
- The CPoC Solution Provider is accountable for managing changes (i.e., change impact, versioning, CPoC Lab integration testing and validation, etc.) including those changes made by third parties that utilize the libraries or API. For example, if a third party develops and manages their own user interface to interface the listed CPoC Solution via the Solution provider's libraries or API, it must not be possible for changes to the user interface to impact any of the CPoC security requirements. The

> ***Note:*** *Any change to the CPoC 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 CPoC Solutions.*

CPoC Solution Provider is responsible for the Solution's security including any impactful changes.

- If a CPoC Solution Provider optionally provides libraries or an API to allow third parties to interface the listed CPoC Solution, the libraries or API is part of *only* the CPoC Solution with which it was Evaluated, validated and listed on the PCI SSC website. Third parties are not permitted to use the libraries or API as part of another CPoC Solution.

Appendix E Software Versioning Methodology

Changes to production-level code require updates to the respective software application's version numbering. Vendors must document and follow a software-versioning methodology as part of their system development lifecycle; the software-versioning methodology may be a separate document or part of the Vendor's *Security Policy*. Additionally, CPoC Application Vendors must communicate the versioning methodology to their customers in their implementation guidance documents. Customers require this information to understand which version of the application they are using and the types of changes that have been made to each. CPoC Labs must verify that the Vendor is adhering to their documented versioning methodology and the requirements of the *CPoC Program Guide* as part of the CPoC Evaluation. If the Vendor maintains a separate version-numbering scheme internally, the Vendor must document and maintain a method to map the internal version numbers to the publicly-listed version numbers. For more information, See *CPoC Standard*, Appendix D, "Software Security Requirements" (item D.1.9).

Version Number Format

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

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

Version Number Usage

All impactful changes[1] to the CPoC Application (and/or its Monitoring/Attestation System) must result in a new application version number. However, whether this affects the version number listed on the Website depends on the nature of the change and the Vendor's published versioning policy. All changes that impact security functionality and/or any CPoC security requirements must result in a change to the version number listed on the Website.

The Vendor 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, etc.
- Changes that do not impact the function of the application or its dependencies
- Changes that impact the application function, but do not impact security or compliance with the *CPoC Standard*
- Changes that impact any security function or compliance with the *CPoC Standard*

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

If the Vendor uses a versioning scheme that involves mapping 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 must be consistent with the versioning policy described in the applicable implementation guides.

Vendors must ensure traceability between application changes and version numbers such that a customer can determine the changes that are included in the version of the application they are running.

[1] See **Error! Reference source not found.**for an overview of the various change types.

Appendix F Terminology

For purposes of this *Program Guide*, the following terms have the meanings set forth below.

***Note:** Additional definitions for PCI terminology are provided in the general PCI Glossary on the PCI SSC Website at www.pcisecuritystandards.org/pci_security/glossary.*

Term	Definition / Source / Document Reference
Accepted/Acceptance	A CPoC Solution is deemed to have been "Accepted" (and "Acceptance" is deemed to have occurred) and will be listed on the List of Validated CPoC Solutions on the Website when PCI SSC has: • Received the corresponding compliant Solution *Evaluation Report* from the CPoC Lab; • Received the corresponding fee and all documentation required with respect to that CPoC Solution as part of the CPoC Program; and • Confirmed that: – The respective compliant Solution *Evaluation Report* is correct as to form (all applicable documents completed appropriately/sufficiently); – The CPoC Lab properly determined that the Solution is eligible to be a validated Solution; – The CPoC Lab adequately reported the compliance of the respective CPoC Solution with CPoC 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 CPoC Program policies and procedures.*
Assessment	On-site assessment of a CPoC Solution's Back-end Monitoring Environment to validate compliance with the *CPoC Standard* as part of the CPoC Program.
Assessor	A CPoC Lab or a QSA Company.
Back-end Monitoring Environment	The secure facility or environment assessed onsite by a CPoC Lab (or QSA Company, as applicable) in accordance with the *CPoC 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.
COTS	Acronym for commercial off-the-shelf device. See the *CPoC Standard* for additional details.
CPoC Application	All parts of the code, regardless of the execution environment, that is installed and executed on the merchant COTS device for the purposes of accepting and processing account data associated with a contactless transaction. The CPoC API, attestation component and/or a payment application may be incorporated into the CPoC application or may be separate. See the *CPoC Standard* for additional information.

Term	Definition / Source / Document Reference
CPoC Element (or Element)	A CPoC Application (including optional APIs), Monitoring/Attestation System, or Back-end Monitoring Environment validated by a CPoC Lab for use as part of a validated CPoC Solution.
PCI-recognized CPoC Laboratory (or CPoC Lab)	A PCI-recognized Contactless Payments on COTS Laboratory qualified by PCI SSC to perform Evaluations of CPoC Solutions for CPoC Program purposes.
CPoC Program	Refers to PCI SSC's program and requirements for qualification of Assessors, Labs and applicable employees thereof and validation and Acceptance of CPoC Solutions or CPoC Elements, as further described in this document and related PCI SSC documents, policies and procedures.
CPoC Application Programming Interface (or CPoC API)	An optional software component or libraries, developed and provided by the CPoC Solution Provider, to allow third-party developers to interface with the CPoC Solution.
CPoC user guidance document (or API user guidance)	A companion document – provided by the CPoC Solution Provider – with the optional CPoC libraries or API outlining the conditions and how the libraries or API can be used to interface the CPoC Solution. See Appendix D of the *CPoC Program Guide* and the *CPoC Standard* for additional information.
CPoC Standard	The then-current version of (or successor document(s) to the Payment Card Industry *(PCI) Contactless Payments on COTS Security and Test Requirements*, any/all testing procedures, appendices, 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. See the *CPoC Standard* for additional information.
CPoC Solution (or Solution)	The set of components and processes that support the contactless read and protection of account data into a COTS device. At a minimum, the Solution includes the CPoC Application and the ack-end systems and environments that perform attestation, monitoring, and payment processing. See the *CPoC Standard* for additional information.
CPoC Solution Attestation of Validation (or AOV)	An "Attestation of Validation" declaring the Solution validation status against the *CPoC Standard*. The *AOV*, signed by the CPoC Lab and CPoC Solution Provider, is used when validating, revalidating or submitting changes to a Solution.
CPoC Solution Evaluation (or Evaluation)	Evaluation of a Solution by a CPoC Lab for purposes of validating compliance against the *CPoC Standard* as part of the CPoC Program, including but not limited to: • Evaluation of the CPoC Application and supporting Monitoring/Attestation System incorporated therein • Back-end Monitoring Environment and all other elements of the Solution • End-to-end integration evaluation of the overall Solution
CPoC Solution Provider (or Solution provider)	The entity that has overall responsibility for the design, implementation and management of the CPoC Solution including ensuring that the Solution meets all applicable *CPoC security requirements*. CPoC Solution Providers are ultimately responsible for ensuring that all the requirements are met.
CPoC Vendor (or Vendor)	Any of the following: CPoC Solution Provider, CPoC Application and supporting Monitoring/Attestation System Vendor, or Back-end Monitoring Environment provider.

Term	Definition / Source / Document Reference
PCI DSS DESV (or DESV)	Acronym for PCI Data Security Standard Designated Entities Supplemental Validation. See the *PCI Glossary* for additional information.
Delta Evaluation	Partial Evaluation of the Solution, performed against applicable CPoC security requirements, when changes to a Solution are eligible for review under the “Delta Evaluation” change-review process described herein.
Evaluation Report	The CPoC Solution *Evaluation Report* required to be completed by a CPoC Lab during CPoC Solution Evaluations and submitted to PCI SSC for review and Acceptance, following the CPoC Solution *Evaluation Report* Template (available on the Website) and instructions therein. For a Solution to be included on the List of Validated CPoC Solutions on the Website, the corresponding *Evaluation Report* must be submitted to PCI SSC for review and Accepted.
List of Validated CPoC Solutions	The list of Solutions on the Website that have been Accepted by PCI SSC for CPoC Program purposes.
Listing (or Listed)	The listing and related information regarding a Solution on the List of Validated CPoC Solutions.
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 CPoC Lab to have met all applicable CPoC security requirements, and then Accepted by PCI SSC, as long as such Acceptance has not been revoked, suspended, withdrawn or terminated. In the *CPoC 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 CPoC Application executes, thereby delivering a level of software-based tamper detection and response. See *the CPoC Standard* for additional information.
Participating Payment Brand (or Payment Brand)	A global payment card brand or scheme that is also a limited liability company member of PCI SSC (or affiliate thereof).
PAN	Acronym for Primary Account Number, defined in the PCI Glossary.
PCI SSC	Acronym for PCI Security Standards Council, LLC.
PIN	Acronym for Personal Identification Number.
Program Guide	The then-current version of (or successor documents to) this document—the *Payment Card Industry (PCI) Contactless Payments on COTS (CPoC™) 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 Security Assessor (or 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.

Term	Definition / Source / Document Reference
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.
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' CPoC Solution Evaluations.
Validated CPoC Solution	A CPoC Solution that has been assessed by a CPoC Lab to be in scope for the CPoC Program and to have met all CPoC security requirements and then Accepted by PCI SSC, so long as such Acceptance has not been revoked, suspended, withdrawn, or terminated.
Vendor Release Agreement (or VRA)	The then-current and applicable form of release agreement that PCI SSC: • Requires to be executed by CPoC Solution Providers and providers of CPoC Elements (for example, Monitoring/ Attestation System, Back-end Monitoring Environment and/or CPoC Application), as applicable, in connection with the CPoC 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.