



Payment Card Industry (PCI) Key Management and Operations (KMO)™

Program Guide

Version 1.0

For use with PCI KMO Standard Version 1.x

September 2026

Document Changes

Date	Version	Description
September 2026	1.0	Initial release of the PCI Key Management and Operations (KMO) [™] Program Guide

Contents

Document Changes	i
i. Terminology	iv
ii. Related Publications	viii
1 Introduction.....	1
1.1 KMO Standard	1
1.2 KMO Program Overview.....	1
1.3 KMO Services	2
1.3.1 <i>KMO Service Functions and Key Data Types</i>	2
1.4 Updates to Documents and Security Requirements	2
1.5 Technical FAQs	3
2 Roles and Responsibilities.....	4
2.1 KMO Vendors	4
2.1.1 <i>Third-Party Service Providers</i>	5
2.2 KMO Assessor Companies	5
2.3 Customers	6
2.4 PCI Security Standards Council (PCI SSC)	6
2.5 Participating Payment Brands	7
3 KMO Assessment Considerations	8
3.1 KMO Assessments of Not-Yet-Deployed Implementations	8
3.2 KMO Service Types and Submissions	8
3.3 KMO Dependencies and Use by Other Referencing PCI Standards / Programs	8
3.4 Remote Assessments.....	9
3.5 Listed KMO Service Outsourcing Matrix	10
3.5.1 <i>KMO Dependencies and use by other KMO Services</i>	10
3.6 Use of Expired Products and Dependencies	11
3.6.1 <i>Expired Secure Cryptographic Devices (SCD)</i>	11
3.6.2 <i>Expired KMO Services</i>	11
3.6.3 <i>Listed KMO Services with Expired Dependencies</i>	11
4 Overview of the Validation Processes	13
4.1 Prior to an Assessment	13
4.2 Required Documentation and Materials	14
4.3 Assessment Timeframes	14
4.4 KMO Assessors	15
4.5 KMO Assessor Company Fees	15
4.6 Other Services Offered by KMO Assessor Companies	15
4.7 Technical Support During the Assessment	16
4.8 Vendor Release Agreement (VRA)	16
4.9 Access to the Portal.....	16
4.10 Portal Submissions	17
5 Changes to Listed and Validated KMO Services	18
5.1 Administrative Changes to Listed KMO Service	18
5.1.1 <i>Administrative Change Submission Process Overview</i>	18
5.2 Delta Changes to Listed KMO Services	19
5.2.1 <i>Delta Change Submission Process Overview</i>	19

6	Lifecycle for Listed KMO Services	21
6.1	Annual Vendor Attestation of Listed and Validated KMO Services	21
6.1.1	Initial Administrative Expiry Period	23
6.1.2	Secondary Administrative Expiry Period	23
6.1.3	Administrative Expiry	23
6.2	Reassessment Process	24
6.2.1	Listing Expiry	24
7	Program Fees.....	25
8	Security Issue Notification	26
8.1	Notification and Timing	26
8.2	Notification Format	26
8.3	Notification Details	26
8.4	Actions following a Security Breach or Compromise	26
8.5	Withdrawal of Acceptance	27
Appendix A	KMO Services and Acceptance	28
Appendix B	Elements for the List of Validated KMO Services	29
B.1	KMO Vendor Company Name.....	29
B.2	Location(s)	29
B.3	Validated KMO Service Name.....	29
B.4	Listing Reference Number	29
B.5	KMO Service Type	29
B.6	KMO KIF Service Function(s) Provided	29
B.7	Cryptography Supported	30
B.8	Key Injection Supported	30
B.9	Key Data Types Supported	30
B.10	Other KMO Service Dependencies	31
B.11	KMO Standard Version.....	31
B.12	KMO Service Status	31
B.13	KMO Assessor Company	31
B.14	Annual Vendor Attestation Date	32
B.15	Reassessment Date	32
B.16	Notes.....	32

i. Terminology

The following capitalized terms have the meanings set forth below for purposes of this document.

Table 1: Glossary of Terms

Term	Definition
Accepted, Acceptance	A Validated KMO Service is deemed to have been “Accepted” (and “Acceptance” is deemed to have occurred so long as such Acceptance has not been revoked, suspended, withdrawn, or terminated) when PCI SSC has: - Received the corresponding Validated KMO Service submission in the Portal, including the completed ROV, AOV, and all other documentation and information as required by the <i>KMO Standard</i> and KMO Program Requirements, from the KMO Assessor and KMO Assessor Company qualified to perform the KMO Assessment of the KMO Service; - Received the corresponding KMO Program fee for the submission; and - Confirmed that: - the Validated KMO Service submission to the Portal is complete (all applicable documents completed appropriately/sufficiently), and - the KMO Assessor Company properly determined that the KMO Service satisfies the <i>KMO Standard</i> and KMO Program Requirements for a Validated KMO Service.
Administrative Change	A change affecting defined administrative information on the Listing for a Listed KMO Service that is not a Delta Change. See also <i>Delta Change</i>.
Administrative Expiry	The early expiry of a Listed and Validated KMO Service due to Program Requirements not being satisfied, whereby the Validated KMO Service is redesignated as an Expired KMO Service. See also <i>Expired KMO Service</i>.
Annual Vendor Attestation (Annual Attestation)	The annual process required of KMO Vendors to confirm and attest that their Listed and Validated KMO Service continues to adhere to the <i>KMO Standard</i> and Program Requirements.
Attestation of Validation (AOV)	A form determined by PCI for KMO Vendors to declare the validation status and submission type, in the context of this Program, of a Product to the Standard and Program Requirements. See also <i>PCI KMO Attestation of Validation</i> in Section ii Related Publications.
Delta Change	A security-impacting change to a Listed KMO Service that affects defined elements in the associated Listing for that KMO Service that is not an Administrative Change. See also <i>Administrative Change</i>
Expired KMO Service (Expired, Expires, Expiration)	A previously Validated KMO Service on the List of Validated KMO Services that has been redesignated as expired and therefore is no longer considered to be a Validated KMO Service, Accepted, or Listed.

Term	Definition
Full Assessment	A complete assessment and validation of a KMO Service by a qualified KMO Assessor Company in accordance with the <i>KMO Standard</i>, Program Requirements, and all associated documentation that results in a Validated KMO Service. A Full Assessment is not an: • Administrative Change, or a • Delta Change A New Assessment and a Reassessment both require a Full Assessment. See also <i>New Assessment</i>, <i>Reassessment</i>.
KMO Assessment (Assessment, PCI KMO Assessment)	Refer to the <i>PCI Qualification Requirements for KMO Assessors</i>
KMO Assessor Company (Assessor Company)	Refer to the <i>PCI Qualification Requirements for KMO Assessors</i>
KMO Assessor Employee (Assessor Employee)	Refer to the <i>PCI Qualification Requirements for KMO Assessors</i>
KMO Program Documents (Program Documents)	The <i>KMO Standard</i> and <i>KMO Program Guide</i> , <i>KMO Qualification Requirements</i> , all written agreements executed between PCI SSC and KMO Vendors, and PCI SSC and KMO Assessors (Companies & Employees) in connection with the KMO Program, all other materials, requirements, obligations, policies, and procedures published from time to time by PCI SSC on the Website or elsewhere relating to the KMO Program, and all successor versions of the foregoing, in each case, as amended from time to time.
KMO Program Guide	The then-current version of (or successor documents to) this document – the <i>Payment Card Industry (PCI) Key Management and Operations (KMO)™ Program Guide</i> , as from time to time amended and made available on the Website.
KMO Program (Program)	The PCI SSC program for Key Management and Operations whereby an entity can choose to have their KMO Service validated by a qualified KMO Assessor (further described in the <i>KMO Qualification Requirements</i>) and subsequently submitted to PCI SSC for consideration of being Accepted and Listed for purposes of demonstrating compliance with the <i>KMO Standard</i> and Program Requirements.
KMO Program Requirements (Program Requirements)	All requirements, obligations, policies and procedures for KMO Services, KMO Vendors and KMO Assessors, as applicable, and as set forth in the corresponding KMO Program Documents, the <i>VRA</i> or otherwise established by PCI SSC from time to time in connection with the KMO Program, including without limitation, those relating to disclosure, PCI SSC's quality assurance initiatives, and/or export control and administration, and such KMO Vendor's warranties pursuant to the <i>VRA</i> .
<i>KMO Report on Validation</i> (or <i>KMO ROV</i> or <i>ROV</i>)	Mandatory template(s) provided by PCI SSC that requires completion by a KMO Assessor Company as part of the validation effort of a KMO Service as per the Program Requirements. See also <i>ROV</i> in the Section <i>ii Related Publications</i>.

Term	Definition
KMO Service	A service of a type that is eligible to be assessed and validated to the <i>KMO Standard</i> and Program. For eligible service types refer to Section 1.3 KMO Services .
<i>KMO Standard</i>	The then-current version of (or successor document(s) to) the <i>Payment Card Industry (PCI) Key Management and Operations Standard</i> , any and all 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 also <i>KMO Standard</i> in Section ii Related Publications .
List of Validated KMO Services	The Council's authoritative List of Validated KMO Services appearing on the Website. The List of Validated KMO Services is the authoritative source of on-going Acceptance by PCI SSC of Validated KMO Services. This list also denotes previously Validated KMO Services that have been redesignated as Expired KMO Services in accordance with Program Requirements and therefore are no longer considered to be Validated KMO Services, Accepted, or Listed. See also <i>Expired KMO Service</i> .
KMO Vendor (Vendor)	An entity that designs, implements, and manages a KMO Service.
Listed	A Validated KMO Service published on the Website after corresponding Acceptance has occurred, so long as such Acceptance has not been revoked, suspended, withdrawn, terminated, or Expired. See also <i>List of Validated KMO Services, Acceptance</i> .
Listing	A unique record for a KMO Service appearing on the List of Validated KMO Services after Acceptance has occurred that contains information as described in Appendix A herein.
New Assessment	A Full Assessment of an eligible KMO Service where that KMO Service: • Is not already a Listed and Validated KMO Service, or • Is an Expired KMO Service See also <i>Reassessment</i> .
Participating Payment Brand (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.
PCI SSC (or the Council)	Refers to the PCI Security Standards Council, LLC.
Portal	PCI SSC's website function that is used to accept PCI Program-related submissions.
Primary Contact	Refer to the <i>PCI Qualification Requirements for KMO Assessors</i> .
Reassessment	A Full Assessment of a Listed KMO Service to the <i>KMO Standard</i> and Program Requirements where that KMO Service is not an Expired KMO Service. See also <i>New Assessment</i> .
Reference Number	A unique identifier assigned to a Validated KMO Service upon Acceptance and denoted on its Listing per the Program Requirements.

Term	Definition
Third-Party Service Provider	An entity that provides a service or function on behalf of a KMO Vendor, which is incorporated into and/or referenced by the applicable KMO Service. A Third-Party Service Provider is only considered a KMO Vendor for eligible KMO Services if the applicable service is separately Listed on the List of Validated KMO Services. A Third-Party Service Provider that does not have a Listed KMO Service must have its services reviewed during the course of each of its customers' KMO Assessments.
Validated KMO Service	A KMO Service that has undergone a Full Assessment by a KMO Assessor Company that satisfies the <i>KMO Standard</i> and Program Requirements, as documented in the corresponding ROV, AOV, and all other associated supporting material and information. Note: A Validated KMO Service requires Acceptance by PCI SSC per the Program to be Listed. See also <i>Listed</i>, <i>Listing</i>, <i>Acceptance</i>. See also <i>List of Validated KMO Services</i>.
Vendor Release Agreement (VRA)	The then-current and applicable form of vendor release agreement that: (a) PCI SSC requires to be executed by KMO Vendors in accordance with the Program Requirements, and (b) Is available on the Website. See also VRA in Section <i>ii Related Publications</i>.
Website	The then-current PCI SSC website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org.

ii. Related Publications

This KMO Program Guide shall be used in conjunction with the latest versions of (or successor documents to) the following PCI SSC publications, each as available through the Website. Related Publications are italicized within this document.

Document	Description
<i>Payment Card Industry (PCI) Key Management and Operations (KMO)™ Requirements and Test Procedures (“KMO Standard,” “PCI KMO Standard”)</i>	Contains the requisite security requirements and associated test requirements for KMO Assessments of KMO Services.
<i>PCI KMO Technical FAQs for use with PCI KMO version 1.x (“KMO Technical FAQs”)</i>	Technical FAQs are an integral and mandatory part of the <i>KMO Standard</i> and Program. Technical FAQs must be fully considered during a KMO Assessment.
<i>PCI Key Management and Operations (KMO)™ Template for Report on Validation (“ROV,” “KMO ROV”)</i>	Mandatory template(s) used by KMO Assessors for validating a KMO Service.
<i>PCI Key Management and Operations (KMO)™ Attestation of Validation (“AOV”)</i>	A form for KMO Assessor Companies and/or KMO Vendors, as required, to attest to the validation status of a KMO Service and the specific submission type to PCI SSC.
<i>PCI Key Management and Operations (KMO)™ Assessor Qualification Requirements (“KMO Qualification Requirements”)</i>	The minimum requirements and related documentation that a KMO Assessor Company and KMO Assessor Employees must satisfy and provide to PCI SSC in order to qualify to perform KMO Assessments as a participant in the KMO Assessor Program.
<i>Vendor Release Agreement (“VRA”)</i>	Establishes the terms and conditions under which validated KMO Service are Accepted and Listed by PCI SSC.
<i>PCI Key Management and Operations (KMO)™ Change Impact Template (“Change Impact Template”)</i>	Mandatory template to account for and submit Administrative Changes and Delta Changes to listed KMO Services.
<i>PCI SSC Remote Assessment Guidelines and Procedures</i>	Describes how remote assessment methods may be incorporated into practices for validating environments, solutions, and products to PCI SSC standards.
<i>PCI PIN Transaction Security (PTS) Device Testing and Approval Program Guide (“PTS Program Guide,” “Device Testing and Approval Program Guide”)</i>	Provides program information for the PCI SSC PTS program, including program information for PCI PTS POI devices and PCI PTS HSMs.

1 Introduction

Note: Capitalized terms used, but not otherwise defined herein, have the meanings set forth or referenced in Section [1 Terminology](#), or in the KMO Standard or KMO Qualification Requirements (each as available on the Website), as applicable.

This document, the *Payment Card Industry (PCI) Key Management and Operations (KMO)™ Program Guide (KMO Program Guide)*, provides information on the PCI KMO Program (the Program) operated and managed by the PCI Security Standards Council, LLC (PCI SSC).

The *KMO Program Guide* is intended for KMO Assessor Companies and KMO Vendors of KMO Services.

Note: Information regarding the qualification of KMO Assessor Companies and their Assessor-Employees can be found in the KMO Qualification Requirements on the Website.

1.1 KMO Standard

The *KMO Standard* details the security and test requirements that a KMO Service must satisfy to be considered a Validated KMO Service by a KMO Assessor that can be considered for Acceptance and Listing by PCI SSC for Program purposes. Validated KMO Services that have been Accepted by PCI SSC are identified on PCI SSC's List of Validated KMO Services on the Website.

1.2 KMO Program Overview

A KMO Vendor may choose to have its KMO Service validated to the *KMO Standard* as part of the Program in order to have the KMO Service considered for Acceptance by PCI SSC and included in the applicable List of Validated KMO Services on the Website.

Refer to Section [1.3 KMO Services](#).

- Applicable KMO Services can be independently validated by a KMO Assessor and Listed on the Website, based on the available options for KMO Service types (detailed in Section [Error! Reference source not found. Error! Reference source not found.](#)). Eligible Listed and Validated KMO Services may also be used as part of other KMO Services or by other referencing PCI Standards / Programs such as PCI P2PE. Refer to Section [3.5 KMO Dependencies and use by other KMO Services](#) for details.
- The KMO requirements and test procedures (sourced from the *KMO Standard*) for validating KMO Services can be found in the corresponding *KMO Report on Validation (ROV)* template(s) found on the Website.
- For each KMO Service to be considered for acceptance by PCI SSC and subsequently Listed on the Website as a Validated KMO Service, Vendors must also submit a *KMO Report on Validation (ROV)*, *PCI KMO Attestation of Validation (AOV)*, acceptance fees, *Vendor Release Agreements (VRAs)*, and other supporting documents, as applicable and described herein.
- Listed and Validated KMO Services must undergo an Annual Vendor Attestation process. Refer to Section [6.1 Annual Vendor Attestation of Listed and Validated KMO Services](#) for further details.

- Any changes made to a Listed and Validated KMO Service must be assessed as to the impact of the change on the ability of that KMO Service to continue to satisfy applicable KMO Program Requirements. Refer to Section [5 Changes to Listed and Validated KMO Services](#) for further details.
- A Reassessment is required on all listed KMO Services every three years based on the Acceptance date of each listing. Refer to Section [6.2 Reassessment Process](#) for further details.
- For a mapping of the requirements of the *KMO Standard* to all KMO Services, refer to the *KMO Standard* document.

Note: PCI SSC reserves the right to require revalidation due to changes to the KMO Standard and/or due to specifically identified vulnerabilities in Listed KMO Services.

1.3 KMO Services

The following are the KMO Services that may be considered for Listing:

- Decryption Management (DM)
- PIN Processing Service (PPS)
- Certificate Authority / Registration Authority (CA/RA)
- Key Injection Facility (KIF)
- Signing Service (SSP)
- HSM-as-a-Service (HaaS)

Notes: KMO Services may be outsourced to other KMO Services. Further details on outsourcing may be found in Section [3.5 Listed KMO Service Outsourcing Matrix](#). KMO listings may be used by other referencing PCI Standards / Programs. Refer to Section [3.3 KMO Dependencies and Use by Other Referencing PCI Standards / Programs](#).

1.3.1 KMO Service Functions and Key Data Types

KMO KIF Service types may be Listed as providing one or more of the following functions.

- Key Generation
- Key Loading
- Management of Key Constituent Material

Each of the above functions may be used by other KMO Services (as part of outsourcing). Refer to Section [3.3 KMO Dependencies and Use by Other Referencing PCI Standards / Programs](#).

Each KMO Service may support key data types (refer to Section [B.9 Key Data Types Supported](#)) for use by other referencing PCI Standards / Programs.

1.4 Updates to Documents and Security Requirements

The *KMO Program Guide* is reviewed regularly and may be modified to reflect continual improvement and quality management of the KMO Program.

PCI SSC reserves the right to add, change, amend, or withdraw security requirements, test requirements, guidance, training, or other requirements at any time.

PCI SSC may provide interim updates to the PCI community through a variety of means, including required training, e-mail bulletins and newsletters, frequently asked questions (which may include technical / normative FAQs), the Website, and other communication methods.

If change to the Program is required, PCI SSC endeavors to work closely with stakeholders to help minimize the impact.

1.5 Technical FAQs

The *PCI KMO Technical FAQs* provide answers to questions regarding the *KMO Standard* and Program. The *KMO Technical FAQs* are a separate document from the *KMO Standard* and are effective immediately upon publication.

Technical FAQs are an integral and mandatory part of the *KMO Standard* and Program. Technical FAQs must be fully considered during a PCI KMO Assessment.

The *PCI KMO Technical FAQs* document can be found in the PCI SSC's Document Library on the Website at https://www.pcisecuritystandards.org/document_library.

2 Roles and Responsibilities

This section provides an overview of the roles and responsibilities of the primary KMO stakeholder groups.

2.1 KMO Vendors

Note: *The decision to undergo an assessment of a KMO Service in pursuit of Acceptance by PCI SSC and subsequent Listing of the Validated KMO Service on the Website is a business decision of the KMO Vendor.*

KMO Vendors seeking Acceptance and subsequent Listing of their Validated KMO Service as part of the Program are entities that are responsible for each of the following:

- Providing access to their KMO Service and supporting documentation to a KMO Assessor Company for validation;
- Ensuring the KMO Service submitted for validation under the Program satisfies all applicable requirements of the *KMO Standard* and Program;
- Complying with the *VRA*, including the adoption and implementation of Vulnerability Handling Policies (defined in the *VRA*) consistent with industry best practices;
- Authorizing the KMO Assessor Company to submit the resulting *ROV*, an *AOV*, and all other required information and documentation for the submission to PCI SSC;
- Paying all invoices from PCI SSC in a timely fashion; and
- Staying up to date with the *KMO Standard* and Program documents, statements, and guidance on the Website.

Only KMO Services validated by a KMO Assessor Company and Accepted on an “Individual basis” by PCI SSC are separately Listed on the Website.

“Individual basis” here refers to the *ROV* for each KMO Service being individually submitted to the Portal. Submissions containing multiple KMO Service types will not be accepted.

To be separately Accepted and Listed, a KMO Service must have its own PCI SSC submission. A separate *ROV* must be submitted to PCI SSC for each KMO Service assessed as part of the Program for it to be Accepted and Listed. If a KMO Service is only assessed as part of another KMO Service that is ultimately Listed, and does not have its own separate Listing on the List of Validated KMO Services, the KMO Service that is not separately Listed (the “Third-Party Service”) is not a Validated KMO Service for Program purposes, and the entity providing the Third-Party Service is considered a Third-Party Service Provider with respect to the Listed KMO Service. A Third-Party Service Provider must have its KMO Services reviewed during the course of each of its KMO Vendor customers’ KMO Assessments.

KMO Assessor Companies are qualified to perform KMO Assessments of KMO Services for consideration of Acceptance by PCI SSC and subsequent inclusion on the List of Validated KMO Services. For eligible KMO Services refer to Section [1.3 KMO Services](#).

The *KMO Report on Validation (ROV)* must be used to validate KMO Services.

2.1.1 Third-Party Service Providers

A KMO Vendor may choose to manage their KMO Service without outsourcing to Third-Party Service Providers.

Alternatively, a KMO Vendor may choose to outsource certain services that are part of their own applicable KMO Service to Third-Party Service Providers, who perform these outsourced, Third-Party Services on behalf of the KMO Vendors.

All KMO-related services performed by Third-Party Service Providers on behalf of a KMO Vendor must be validated per applicable *KMO Standard* and Program requirements as part of the validation of the KMO Vendor's KMO Service. Third-Party Service Providers also have the option of having their services validated independently under the Program.

There are two validation options for Third-Party Service Providers performing KMO functions on behalf of KMO Vendors:

- Undergo a KMO Assessment of the applicable KMO Service against relevant KMO requirements and test procedures (sourced from the *KMO Standard*) and have their KMO Assessor Company submit the applicable *KMO Report on Validation (ROV)* to PCI SSC for review and Acceptance. Upon Acceptance, the corresponding KMO Service is Listed on PCI SSC's List of Validated KMO Services.
- Have their services reviewed during and as part of each of their customers' corresponding KMO Assessments.

Accordingly, a KMO Service can be reviewed via the following scenarios:

- A KMO Vendor can outsource services to Third-Party Service Providers and have the services assessed as part of the overall KMO Assessment of that KMO Service; and/or
- A KMO Vendor can outsource certain functionality to eligible Listed KMO Services and report the use of those Listed KMO Service in its ROV. Refer to Section [1.3.1 KMO Service](#) and Section [3.5 Listed KMO Service Outsourcing Matrix](#).

KMO Vendors must manage the overall KMO Service and any Third-Party Services (and corresponding Third-Party Service Providers) used to perform KMO-related services on their behalf, whether those Third-Party Services are separately Listed by PCI SSC as Validated KMO Services or are assessed as part of the KMO Assessment of the corresponding KMO Service.

The KMO Assessor is responsible for confirming that the scope of any services outsourced to a Listed KMO Vendor is wholly and appropriately covered by the Listed KMO Service.

Note: Pursuant to the VRA, KMO Vendors must ensure that all Third-Party Service Providers are subject to the contractual and operational requirements applicable under the VRA, including, where applicable, requirements relating to vulnerability handling, security issue notification, and authorization for the Vendor to disclose relevant information to PCI SSC.

2.2 KMO Assessor Companies

KMO Assessor Companies are qualified by PCI SSC to perform KMO Assessments of KMO Services. KMO Assessor Companies are responsible for:

- Performing KMO Assessments of KMO Services in accordance with the *KMO Standard*, the KMO Program, and the *KMO Qualification Requirements*.

- Determining the scope of their KMO Assessments and applicability of the *KMO Standard* to each of those KMO Assessments.
- Assessing the compliance of KMO Services against the *KMO Standard* and Program.
- Documenting each KMO Assessment using the applicable *ROV Templates (ROV)*.
- Submitting the applicable *ROV(s)* or any change submission to PCI SSC, along with the applicable *AOV* signed by both the KMO Assessor Company and KMO Vendor.
- Maintaining an internal quality assurance process for their KMO Assessment efforts.
- Staying up to date with PCI SSC statements and guidance, *KMO Technical FAQs*, industry trends, and best practices.

As indicated above, PCI SSC does not approve *ROVs* from a technical compliance perspective, but performs quality assurance to confirm that *ROVs* adequately document the demonstration of compliance.

2.3 Customers

Customers seeking to use Validated KMO Services are responsible for selecting a Validated KMO Service from the List of Validated KMO Services on the Website.

2.4 PCI Security Standards Council (PCI SSC)

Note: *PCI SSC does not manage security standards compliance programs and does not impose any consequences for non-compliance with security standards. Whether an entity is required to comply with or validate compliance to a PCI SSC standard is at the discretion of the organization that manages its own compliance program(s), such as a Payment Brand, acquirer, or other entity.*

PCI SSC is the standards body that develops and maintains the PCI standards. In relation to the KMO Program, PCI SSC:

- Hosts the List of Validated KMO Services on the Website;
- Provides training for and qualifies KMO Assessor Companies and KMO Assessors to perform KMO Assessments;
- Lists KMO Assessor Companies on the Website;
- Maintains and updates the *KMO Standard* and Program, and related documentation according to a standard's lifecycle management process; and
- Reviews all Program submissions to PCI SSC for adherence with baseline quality standards, including but not limited to, confirmation that:
 - Submissions (including *ROVs*, Change Impact Submissions, and Annual Vendor Attestations) are correct as to form;
 - The KMO Assessor Company determines whether KMO Services are eligible for validation under the KMO Program (PCI SSC reserves the right to reject or remove the applicable Listing of any Validated KMO Service determined to be ineligible for the KMO Program);
 - The KMO Assessor Company adequately reports the assessment findings of the Validated KMO Service in their associated submissions; and
 - Details provided in such submissions meet PCI SSC's reporting requirements.

- As part of the PCI SSC quality assurance (QA) process, PCI SSC assesses whether overall, a KMO Assessor Company's operations appear to conform to PCI SSC's quality assurance and qualification requirements.

Note: PCI SSC does not assess or validate KMO Services; assessment and validation is the role of the KMO Assessor Company and its KMO Assessors qualified to evaluate KMO Services to the KMO Standard and Program. Listing of a Validated KMO Services on the List of Validated KMO Services signifies only that the applicable KMO Assessor Company has determined that the KMO Service is in accordance with the KMO Standard and Program Requirements, that the KMO Assessor Company has submitted the corresponding ROV and all associated documentation and information to PCI SSC, and that everything submitted to PCI SSC has satisfied all Program Requirements as of the time of PCI SSC's review.

2.5 Participating Payment Brands

The Participating Payment Brands independently develop and enforce the various aspects of their respective compliance programs, including but not limited to, related requirements, mandates, and due dates.

3 KMO Assessment Considerations

The following section provides information and applicable criteria related to defined KMO Service elements and/or dependencies that must be considered for KMO Assessments.

3.1 KMO Assessments of Not-Yet-Deployed Implementations

A KMO Assessment may be performed for implementations where some or all aspects of the KMO Assessment are not yet deployed. Examples of this include where a KMO KIF Service has all physical, logical, and procedural items in place, but where past evidence of key loading processes do not yet exist as the KMO KIF Service has not yet begun operations.

In these cases, the KMO Assessor may proceed to validate whether the KMO Vendor, and their KMO KIF Service meets the applicable KMO requirements and test procedures (sourced from the *KMO Standard*) by assessing example or test operations. In each case where a KMO Assessor has validated a requirement in this way, this must be documented in the *ROV* requirement finding detail as 'not-yet-deployed.'

Items which may be considered as acceptable for this type of validation include only evidence of past operations. A requirement may not be validated under the not-yet-deployed process if it is required for initial operations. This includes all physical, logical, and procedural documentation requirements.

Any KMO Assessment that includes not-yet-deployed findings is required to have a KMO Assessor perform a Reassessment of these items to confirm they are all "In-Place" no more than 3 years after the not-yet-deployed finding is made. Any not-yet-deployed finding that is unable to be found "In-Place" after 3 years since the not-yet-deployed finding is made is to be marked as "Not In-Place," or "N/A" if the aspect is non-mandatory and can be removed from the scope of the KMO Vendor's KMO Assessment (e.g., if a KMO KIF Service is unable to provide evidence of compliant key generation, the KMO KIF Service may remove key generation from the services they provide).

A not-yet-deployed finding cannot be made for keys that are owned by the KMO Vendor under KMO Assessment. For example, a KMO Vendor cannot have a not-yet-deployed finding for the keys they rely on as part of their own HSM implementation (e.g., such as the HSM master key). Equally, a not-yet-deployed finding cannot be used in substitution of a "Not In-Place" finding – if evidence exists, but does not support an "In-Place" finding, the *ROV* must mark that requirement as "Not In-Place."

3.2 KMO Service Types and Submissions

A KMO Assessment may cover more than one KMO Service for any single entity and assessment. For example, a single KMO Assessment may be performed and submitted to indicate a single KMO Vendor provides both KIF and PPS KMO Services.

3.3 KMO Dependencies and Use by Other Referencing PCI Standards / Programs

KMO may be utilized or relied upon by other referencing PCI Standards / Programs either by the other program referencing an existing KMO Listing, or by the other program using the *KMO Standard* as part of the overall assessment to the other referencing PCI Standard / Program (without relying on a separate KMO Listing).

When used as part of another referencing PCI Standard / Program, a KMO submission is not necessary under the KMO Program – the other program will detail how the details of the validation against the *KMO Standard* are to be submitted to PCI SSC. This may involve a *KMO ROV* being submitted as part of that other standard/program, or it may involve some other process as defined by that other program.

A KMO submission can itself reference other KMO Listings – for example a Listed PPS KMO Service can reference one or more Listed KMO KIF Services, and a KIF can reference another KIF, etc. Refer to Section [1.3.1 KMO Service](#), and Section [3.5 Listed KMO Service Outsourcing Matrix](#).

Acceptance and subsequent inclusion of KMO Services on the List of Validated KMO Services depends on eligibility and is optional. However, such independent Listing is required for a given KMO Service to be recognized as a Validated KMO Service that can be used by other KMO Services and/or other referencing PCI Standards / Programs without the need for a Full Assessment of the applicable KMO requirements and test procedures (sourced from the *KMO Standard*) each time they are used with a different KMO Service and/or referencing PCI Standard / Program.

For KMO Assessments (of KMO Services that use other KMO Services):

- If a KMO Service is currently Listed on the List of Validated KMO Services, the applicable *KMO ROV* has already been Accepted by PCI SSC. As a result, any Listed KMO Service referenced by another KMO Service (the referencing KMO Service) or by another solution in connection with satisfying the requirements under another referencing PCI Standard / Program only needs to be identified in the *KMO ROV* or the applicable reporting method of the other PCI Program, respectively, and an assessment of that already-Listed KMO Service is not required as part of the referencing KMO Service or other PCI Program submission.
- If a KMO Service that is included in a referencing KMO Service submission, or other referencing PCI Standard / Program submission, is not already on the List of Validated KMO Services, but is being submitted to PCI SSC for Acceptance and Listing on the List of Validated KMO Services, the applicable *KMO ROV* must be submitted to PCI SSC for review and Accepted before the ROV of the referencing KMO Service or other PCI Program in which the referencing KMO Service is included can be Accepted.

If independent Listing is not being pursued for a KMO Service, this is instead considered a part of a monolithic assessment for some other referencing PCI Standard / Program, and the ROV is to be included in the submission of that other referencing Standard/Program submission, as required by the program requirements of that other referencing PCI Standard / Program.

3.4 Remote Assessments

If remote assessment methods are used in place of an onsite KMO Assessment, the KMO Assessor must complete the *Addendum for ROC/ROV: Remote Assessments (the “Remote Assessment Addendum”)* as provided in Appendix A of the *PCI SSC Remote Assessment Guidelines and Procedures*, as part of the submission to PCI SSC.

Incomplete findings are to be marked as “Not In-Place.”

A Remote Assessment Addendum must be completed for each KMO Assessment in which an on-site activity is performed remotely that the KMO Assessor determines has the potential to warrant additional consideration to achieve an equivalent confidence level.

One of the most relevant examples is a physical in-person inspection of a physical environment, or in-person observation of processes being conducted within a physical environment. Remote methods in this context warrant the use of the Remote Assessment Addendum.

However, the following activities alone may not warrant the use of the Remote Assessment Addendum, unless the Assessor determines the activity has the potential to warrant additional consideration to achieve an equivalent confidence level as stated prior:

- Documentation review
- Vendor personnel interviews

3.5 Listed KMO Service Outsourcing Matrix

Note: Refer to Section 1.3 KMO Services for all of the KMO Service categories.

The KMO Standard and Program provide significant flexibility in allowing the use of Listed and Validated KMO Services to assist in satisfying the program requirements for a referencing PCI Standard / Program (as described in Section 3.3 KMO Dependencies and Use by Other Referencing PCI Standards / Programs) or the KMO Program Requirements (Section 3.5.1 KMO Dependencies and use by other KMO Services).

3.5.1 KMO Dependencies and use by other KMO Services

The following matrix indicates the allowable Listed and Validated KMO Services that can be included in a KMO Service undergoing validation. While the use of Listed and Validated KMO Services in a KMO Assessment is optional, all requisite requirements must be satisfied by the KMO Service under assessment. Refer to the KMO Standard, Table 3. KMO Service Applicability Matrix.

Figure 1: Listed KMO Services Outsourcing Matrix

Outsourcing Matrix		Listed KMO Service Categories					
		DM	PPS	KIF	SSP	CA / RA	HaaS
Under Assessment	DM	✓	⊘	✓	✓	✓	✓
	PPS	⊘	✓	✓	✓	✓	✓
	KIF	⊘	⊘	✓	⊘	✓	✓
	SSP	⊘	⊘	⊘	✓	✓	✓
	CA / RA	⊘	⊘	⊘	⊘	✓	✓
	HaaS	⊘	⊘	⊘	⊘	⊘	✓

Legend:

- ✓ Allowed
- ⊘ Not Allowed

3.6 Use of Expired Products and Dependencies

3.6.1 *Expired Secure Cryptographic Devices (SCD)*

Where Secure Cryptographic Devices (e.g., POI, HSM) are used with KMO Service(s), the Standard provides details on the acceptable device types and validation. For any currently deployed devices which have an expired or historic listing, the device is considered acceptable for continued use if all of the following are met:

- 1) The KMO Vendor continues to maintain a vulnerability management process to monitor and address any potential security issues with the SCD as required under the Standard. At any point where the SCD is unable to be maintained in a secure state, the SCD is removed from service.
- 2) For any PCI Listed products, the expired listing is not marked as 'Revoked' or 'Withdrawn'.
- 3) For any devices on the CMVP Historical Validation List it is confirmed that the reason for the transition to the CMVP Historical Validation List does not compromise the KMO Service from satisfying applicable KMO Standard requirements.

If any of the above conditions are not met during the PCI SSC AQM review process the submission will be rejected.

Newly deployed PCI Listed products (i.e. devices yet to be loaded with keys and deployed to operational status, or deployed since the previous PCI KMO assessment) are required to have a non-expired listing, with current firmware.

The above rules for handling expired SCD validation apply to both new PCI KMO Assessments, and PCI KMO reassessments for currently deployed devices only. Devices found to meet these requirements during an Assessment or reassessment can continue to be used throughout the associated listing period (and therefore can be considered acceptable during annual attestations).

3.6.2 *Expired KMO Services*

New Assessments and Reassessments of KMO Services will not be Accepted if they use other Expired KMO Services. If at any time prior to Acceptance of the submission, including during the PCI SSC AQM review process, a KMO Service dependency is Expired or Expires, the KMO Service submission will be rejected. If a KMO Service is not on the List of Validated KMO Services, then it must undergo a Full Assessment as part of the assessment and submission process.

3.6.3 *Listed KMO Services with Expired Dependencies*

During the 3-year lifecycle of a Listed KMO Service, underlying Listed KMO Service dependencies denoted within the details of that KMO Service might transition to being Expired.

An Expired KMO Service dependency is not automatically removed from the details of the Listed KMO Service. The parent Listed KMO Service will include an indication that it is using a dependency that is not in accordance with applicable KMO Program Requirements. The Expired KMO Service dependency will be denoted as being Expired in the details of the parent Listed KMO Service.

However, as Expired KMO Services are no longer considered validated, the KMO Vendor is encouraged to promptly remediate any Expired dependencies.

Options for remediating the existence of an Expired dependency will vary depending on the specific KMO Services involved. These options may include, but are not limited to, one or more of the following:

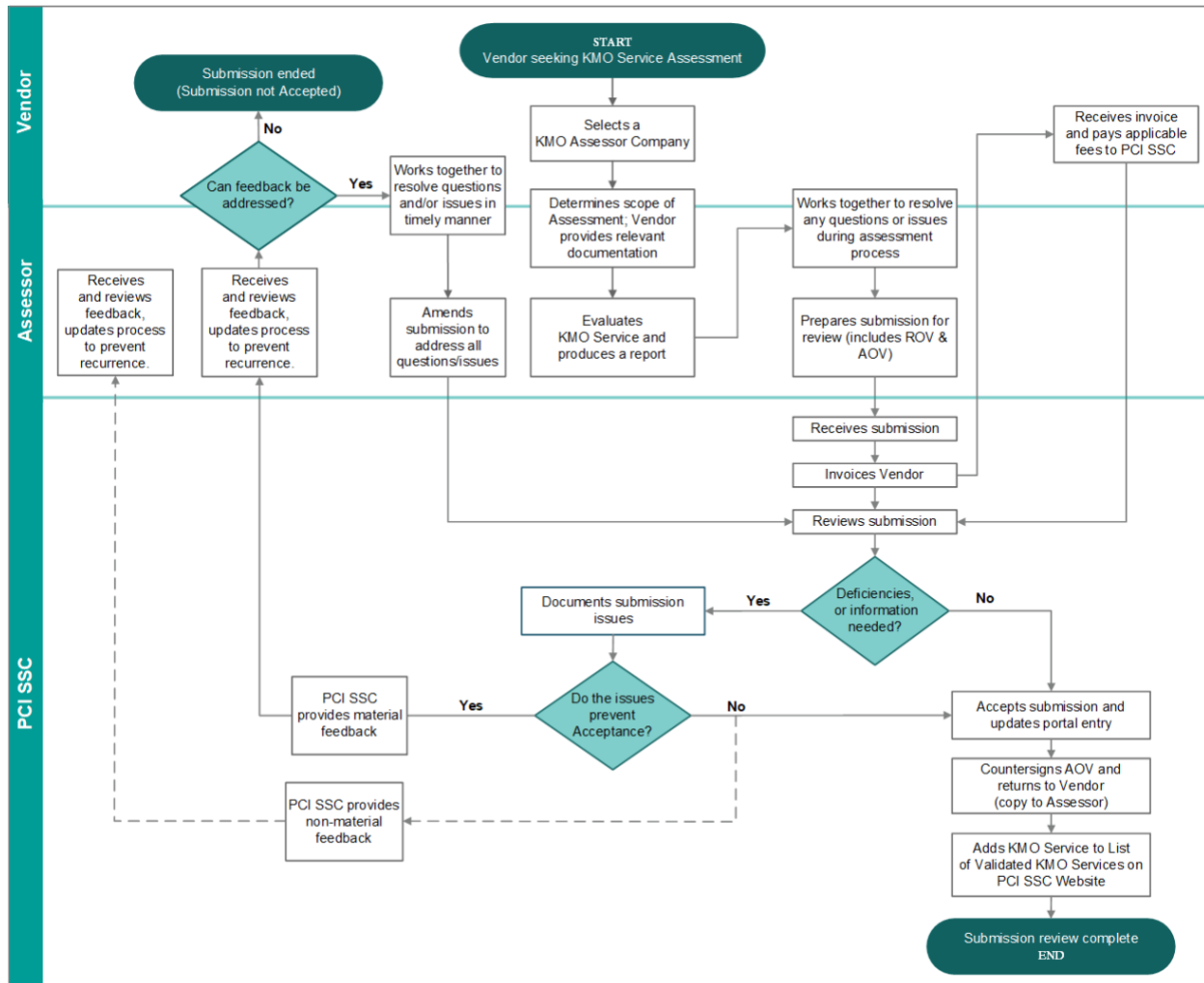
- Discontinuing the use of the Expired dependency and removing it from the Validated KMO Service's Listing.
- Replacing the Expired dependency with a commensurate Validated KMO Service.
- Undergo a KMO Assessment to validate the applicable KMO Program Requirements previously satisfied using the now-Expired KMO Service dependency.

KMO Vendors are encouraged to consult with a KMO Assessor Company to determine the appropriate course of action for your unique situation.

4 Overview of the Validation Processes

The following sections provide a general overview of the validation processes for KMO Services. A general overview of the validation process is as follows:

Figure 2: Validation Process Overview



4.1 Prior to an Assessment

Prior to commencing an Assessment of a KMO Service by a KMO Assessor Company, KMO Vendors are encouraged to take the following preparatory actions:

- Thoroughly review the latest *KMO Standard*, associated *KMO Technical FAQs*, and *KMO Program Guide*, which are all available on the Website.
- Determine if the service intended to be assessed is eligible as a KMO Service that can be validated as per the KMO Program.
- Determine the readiness of the service to satisfy the *KMO Standard* and Program Requirements. This may include the following:

- Perform a gap analysis between the KMO Service and the *KMO Standard's* requirements and test procedures;
- Remediate identified gaps; and
- If desired, a KMO Assessor Company may perform a pre-assessment or gap analysis of a KMO Vendor's KMO Service to help identify deficiencies that require remediation.
- Ensure all the required documentation for the KMO Assessment is accurate and complete.

4.2 Required Documentation and Materials

The KMO Vendor and KMO Assessor work together to account for all KMO Assessment-related materials (such as, but not limited to, *ROV(s)*, *AOV*, the *VRA*, and all other materials related to the KMO Service Assessment and participation in the KMO Program). The KMO Vendor does not submit any documentation directly to PCI SSC as part of a KMO Assessment.

4.3 Assessment Timeframes

The amount of time necessary to perform and complete a KMO Assessment can vary widely depending on factors such as, but not limited to:

- The degree that the KMO Service satisfies the *KMO Standard* and Program Requirements at the start of the Assessment;
 - Corrections to the KMO Service, including required documentation, to remediate gaps will delay the KMO Assessment and validation.
- Prompt payment of applicable fees due to PCI SSC for the Validated KMO Service submission;
 - PCI SSC will not commence the review of the submission until the applicable fees have been paid.
- The scope of the Assessment and validation effort. The use of Listed KMO Services can reduce the scope.

A broader scope of the Assessment will increase the review time of the KMO Service submission.
- Quality of the KMO Assessor Company's submission to PCI SSC;
 - Submissions that are incomplete or contain errors – for example, missing or unsigned documents, incomplete or inconsistent submissions – will result in delays in the review process.
 - If PCI SSC reviews the *ROV* more than once, providing comments back to the Assessor Company to address each time will increase the length of time for the review process.

Any Assessment timeframes provided by PCI SSC or an Assessor Company should be considered estimates. Issues found during the review or Acceptance process, discussions required between the Assessor, the Vendor, and/or PCI SSC, or other matters may significantly impact review times and cause delays and/or may even cause the review to end prematurely (for example, if the Vendor decides it does not want to remediate identified issues or it is determined that the KMO Service is not eligible for validation under the *KMO Standard* and Program).

4.4 KMO Assessors

PCI SSC qualifies and provides required training for KMO Assessor Companies and their KMO Assessor Employees.

PCI SSC qualification authorizes KMO Assessor Companies and their KMO Assessor Employees for Program purposes to perform Assessments to the major version (which includes all associated minor versions) of the *KMO Standard* and Program Requirements for which they have successfully completed training. Refer to the *KMO Qualification Requirements* for details.

- For each KMO Assessment, the resulting report is required to use the *Report on Validation Template (ROV Template)* in unmodified form in accordance with the *KMO Standard* and Program.
- The Assessor Company must prepare and complete each *ROV* based on evidence obtained by following the *KMO Standard* and Program Requirements.
- Prior to submitting to PCI SSC, the Assessor Company must perform a review of all documents to ensure they are consistent and meet PCI SSC's requirements and quality standards.
- Each Validated KMO Service submission to PCI SSC for consideration of Acceptance and Listing must be accompanied by a corresponding *PCI KMO Attestation of Validation (AOV)* in unmodified form available on the Website.

4.5 KMO Assessor Company Fees

KMO Assessor Company prices and fees are set by the KMO Assessor Companies (not by PCI SSC). These fees are negotiated between the KMO Assessor Company and KMO Vendors seeking to have their KMO Service validated to the *KMO Standard* and Program Requirements. Before selecting an Assessor Company, it is recommended that the Vendor check PCI SSC's list of KMO Assessor Companies on the Website, talk to several Assessor Companies, and follow its own Vendor selection processes.

4.6 Other Services Offered by KMO Assessor Companies

Subject to the independence requirements specified in the *KMO Assessor Qualification Requirements*, a KMO Assessor Company may provide other services. If any other services are of interest, contact the KMO Assessor Company for details. Examples of other services may include:

- Providing guidance on designing the service in accordance with the *KMO Standard*;
- Reviewing the Vendor's service, responding to inquiries, clarifying requirements, etc.;
- Providing recommendations on preparing documentation;
- Providing pre-assessment (gap analysis) services prior to beginning a formal Assessment;
- Providing guidance for meeting the *KMO Standard* requirements.

Note: When considering other services with a KMO Assessor Company (including but not limited to those described immediately above), care must be taken by both the Vendor and the Assessor Company to ensure that the Assessor Company maintains all independence requirements as set forth in the *KMO Qualification Requirements* – for example, that a KMO Assessor Company does not, as part of the Assessment, assess its own work product. Conflicts of interest may result in a Vendor's Assessment being rejected by PCI SSC.

4.7 Technical Support During the Assessment

It is recommended that the Vendor designate an individual with sufficient technical knowledge to act as a designated contact throughout the review and assist with any questions that may arise. The Vendor's designated contact should be available to address inquiries from the Assessor Company.

4.8 Vendor Release Agreement (VRA)

For PCI SSC to review any submission, PCI SSC must have on file the Vendor's signed copy of the then-current version of the *Vendor Release Agreement (VRA)* available on the Website.

- If PCI SSC does not have a copy of the Vendor's signed then-current *VRA* on file, the Assessor Company must provide such *VRA* to PCI SSC.
- If PCI SSC does have a copy of the Vendor's signed then-current *VRA* on file, the Assessor Company is not required to re-submit the same *VRA* to PCI SSC at that time.

Generally, the Vendor provides its signed *VRA* to the Assessor Company, along with access to their KMO Service and other documents and materials, at the beginning of the applicable assessment and validation process.

The *VRA*, in part:

- Covers confidentiality issues;
- Covers the Vendor's agreement to KMO Program Requirements, policies, and procedures;
- Gives permission to the Vendor's chosen Assessor Company to release the completed *ROV* and related materials to PCI SSC for review; and
- Requires Vendors to adopt and comply with industry standard Vulnerability Handling Policies.

Note: A submission will not be reviewed by PCI SSC without the then-current *VRA* on file from the relevant Vendor.

4.9 Access to the Portal

Access to the Portal is granted to qualified KMO Assessor Companies. KMO Assessors receive log-on instructions upon passing PCI SSC's KMO Assessor training exam. The Primary Contact for a KMO Assessor Company for Program purposes must be a KMO Assessor and receives higher-level access to the Portal than KMO Assessors who are not the Primary Contact, to enable the Primary Contact to manage Assessor Company-related tasks. Access is granted to the Primary Contact upon e-mail request to the PCI SSC KMO Program Manager at kmo@pcisecuritystandards.org.

Restricted access to the Portal is granted to all KMO Vendor's with a Listed and Validated KMO Service, or upon new KMO submission. This restricted access allows all such Vendor's to submit required Annual Vendor Attestations to complete the required Annual Vendor Attestation processes.

Note: Vendor use of the Portal is subject to payment of applicable Program fees specified in the Fee Schedule for the submission type or activity being performed.

4.10 Portal Submissions

All information and documents required for a Validated KMO Service must be submitted to PCI SSC by the KMO Assessor Company using the Portal (with exceptions noted herein Section [4.9 Access to the Portal](#) and Section [6.1 Annual Vendor Attestation of Listed and Validated KMO Services](#)) for Annual Vendor Attestation submissions by Vendors.

After the invoice for the applicable fees has been paid, PCI SSC will perform an administrative review (“pre-screening”) to ensure that the submission is complete. PCI SSC’s Assessor Quality Management (AQM) will then conduct a complete review of the product submission, including review of the ROV and AOV to ensure reporting quality expectations are met, and the assessor’s findings are adequately supported by referenced evidence. Overall, submitted materials must provide reasonable assurance that the Validation of the KMO Service was performed in accordance with applicable Program Requirements and meets quality standards.

Any inquiries or feedback from AQM will be provided via the Portal and must be addressed by the KMO Assessor Company in a timely manner. It is the responsibility of the Assessor Company to resolve all inquiries and feedback with PCI SSC as applicable.

Quality issues may result in delays in the submission review process by PCI SSC, or potential rejection of the submission if the issues cannot be resolved, either entirely or in a timely manner.

Once the ROV and associated documents meet all applicable quality assurance requirements (as documented or referred to in the *KMO Qualification Requirements* and related KMO Program materials), PCI SSC will send the countersigned AOV to both the KMO Vendor and the Assessor Company and will add the KMO Service to the List of Validated KMO Services.

Note: Findings arising from PCI SSC’s review of Portal submissions may be used by PCI SSC in connection with its ongoing quality assurance and oversight of KMO Assessor Companies under the *KMO Qualification Requirements*.

5 Changes to Listed and Validated KMO Services

KMO Vendors may need to update their Listed KMO Service for various reasons. The Change Impact Template must be used to account for and submit Administrative Changes and Delta Changes to PCI SSC.

Notes:

Changes are permissible only for Listed and Validated (not Expired) KMO Services.

Any change to a Listed KMO Service that is not an Administrative Change and not a Delta Change is accounted for by the KMO Vendor as part of the Annual Vendor Attestation process for the Listed and Validated KMO Service. Refer to Section [6.1 Annual Vendor Attestation of Listed and Validated KMO Services](#) for further details.

Administrative Changes and Delta Changes do not have any impact on Annual Vendor Attestation dates or Reassessment dates of Listed and Validated KMO Services.

5.1 Administrative Changes to Listed KMO Service

Note: *The Change Impact Template on the Website must be used to document Administrative Changes and be provided via the Portal as part of the Administrative Change submission. An AOV in the form provided on the Website is also required.*

An Administrative Change is used to update information on a Listed and Validated KMO Service that does not require a Delta Change submission. This includes:

- KMO Vendor Company Name (requires an updated VRA)
- KMO Service Name

5.1.1 Administrative Change Submission Process Overview

1. The Vendor and the KMO Assessor Company prepare and complete the *Change Impact Template* and corresponding AOV;
2. If the Administrative Change requires an updated VRA, the Vendor completes the then-current VRA and submits this to the Assessor Company;
3. The KMO Assessor Company submits the Administrative Change (and then-current VRA, if applicable) to PCI SSC through the Portal;
4. PCI SSC will then issue an invoice to the Vendor for the applicable change fee; and
5. Upon payment of the invoice, PCI SSC will review the Administrative Change submission.

Following successful PCI SSC quality assurance review of the Administrative Change, PCI SSC will:

1. Amend the Validated KMO Service details on the corresponding List of Validated KMO Services on the Website accordingly based on the Administrative Change submission; and
2. Sign and return a copy of the corresponding AOV to both the Vendor and the KMO Assessor Company. An Administrative Change does not change the associated Annual Vendor Attestation date or Reassessment date.

For quality issues associated with any aspect of the submission, PCI SSC communicates those issues to the KMO Assessor Company. PCI SSC reserves the right to reject any Change Impact

submission if it determines that a change described therein and purported to be an Administrative Change by the KMO Assessor Company and/or Vendor is ineligible for an Administrative Change.

5.2 Delta Changes to Listed KMO Services

Notes:

The assessment of Delta Changes to a Listed and Validated KMO Service must be performed using the same major version of the KMO Standard and Program as were used for the Full Assessment.

Delta Change submissions to add Expired KMO Services will not be Accepted. If at any time prior to Acceptance of the Delta Change submission, including during the PCI SSC AQM review process, a KMO Service being added as part of the Delta Change is Expired or Expires, the Delta Change submission will be rejected. Delta Changes to add KMO Services to an existing Listed and Validated KMO Service without further assessment requires the KMO Service being added to be on the List of Validated KMO Services.

The Change Impact Template on the Website must be used for Delta Changes.

Delta Changes are security-impacting changes (not Administrative Changes) made to a Listed KMO Service as defined and accounted for in the *Change Impact Template* that affect a Listing element as defined in [Appendix B](#). Generally, Delta Changes include, but are not limited to the following:

- Add/remove Listed and Validated KMO Service(s) to an existing Listed and Validated KMO Service. Refer to Section [3.5 Listed KMO Service Outsourcing Matrix](#) and Section [Error! Reference source not found. Error! Reference source not found.](#)
- Add/remove/change KMO Service functions. Refer to Section [1.3.1 KMO Service and Key Data Types](#).
- Add/remove/change Key Data Types Supported. For example, a KMO Assessment may be scoped to assess an implementation of new key data type for an existing Listed and Validated KMO Service. The KMO Vendor of a Listed and Validated PPS KMO Service may choose to support P2PE key data types, and in that case a KMO Assessment may be performed to cover just the differences between the KMO Service as it relates to PIN keys and operations versus P2PE keys and operations. Refer to Section [B.9 Key Data Types Supported](#).

Note: *Delta Changes cannot be used to perform partial assessments of new services.*

5.2.1 Delta Change Submission Process Overview

The Vendor and the KMO Assessor Company prepare and complete the *Change Impact Template*. It is recommended that the Vendor submit the Delta Change request to the same KMO Assessor Company used for the last Full Assessment of the Listed KMO Service.

For changes eligible as a Delta Change under the Program:

1. The Vendor completes a new VRA, if applicable;
2. The Vendor, or the Vendor and KMO Assessor Company where required, determine if the changes qualify as a Delta Change and complete the *Change Impact Template* for the Listed and Validated KMO Service, including all required [re]testing and [re]validation;

3. Additional documents, such as a redlined *ROV*, are completed as instructed in and required by the *Change Impact Template*;
4. The Vendor and KMO Assessor Company prepares and signs the AOV;
5. The KMO Assessor Company submits all required documentation per this Program Guide and applicable KMO Program Requirements to PCI SSC for the Delta Change;
6. PCI SSC will then issue an invoice to the Vendor for the applicable Program fee; and
7. Upon payment of the invoice, PCI SSC will review the Delta Change submission for eligibility, quality assurance purposes, and consistency.

Following successful PCI SSC quality assurance review of the Delta Change, PCI SSC will:

1. Amend the Validated KMO Service Listing details accordingly based on the Accepted Delta Change submission; and
2. Sign and return a copy of the corresponding AOV to the Vendor (and the KMO Assessor Company as applicable). A Delta Change does not change the associated Annual Vendor Attestation dates or the Reassessment date.

PCI SSC reserves the right to reject any submission if it determines that a change described therein and purported to be an eligible Delta Change by the KMO Assessor Company and/or the Vendor is ineligible for a Delta Change.

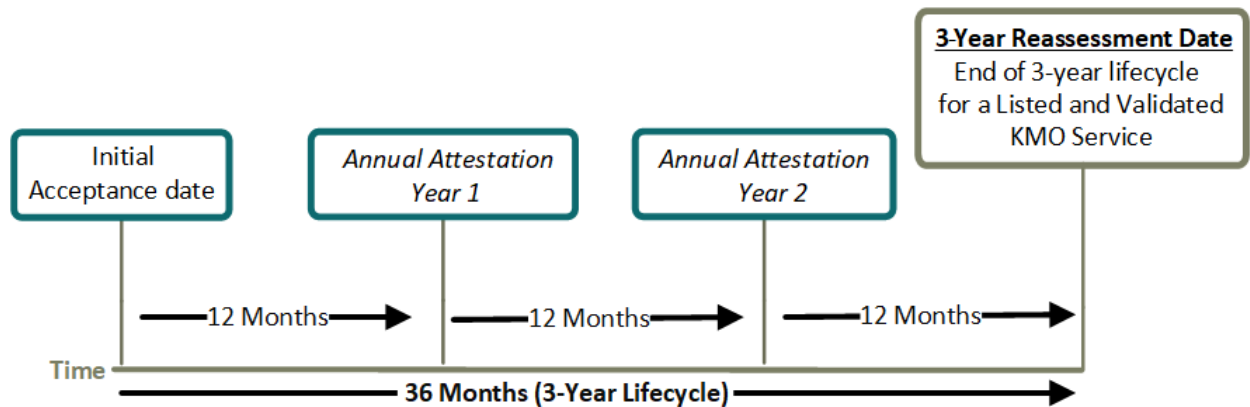
6 Lifecycle for Listed KMO Services

A validated KMO Service, upon Acceptance and being Listed as the result of a Full Assessment, remains Validated for 3 years based on the date of the most recent Acceptance, provided it satisfies the Program Requirements as described herein.

Once Listed, a KMO Service is required to satisfy the Annual Vendor Attestation process at year 1 and year 2 based on the date of the most recent Acceptance.

At the end of the 3-year lifecycle, Vendors have the option of undergoing a Reassessment as described herein to renew the Listing for their KMO Service.

Figure 3: Listed KMO Service 3-Year Lifecycle



6.1 Annual Vendor Attestation of Listed and Validated KMO Services

The Annual Vendor Attestation (Annual Attestation) process requires the Vendor to attest to and account for their Listed and Validated KMO Service continuing to adhere to the *KMO Standard* and Program Requirements via their submittal of the AOV.

The first Annual Attestation is required one calendar year after the most recent date of Acceptance based on the last Full Assessment. If the Vendor satisfied all applicable Program Requirements for the first Annual Attestation, then the second Annual Attestation is required one calendar year after the first Annual Attestation date. If the Vendor did not satisfy all applicable Program Requirements for the first Annual Attestation, then the Listed KMO Service is subject to Administrative Expiry as described in Section [6.1.3 Administrative Expiry](#).

PCI SSC will send a courtesy reminder notification to the Vendor's contact (as identified in the AOV) within 90 calendar days prior to the relevant Annual Attestation date, however it is the sole responsibility of the Vendor to maintain their respective Listing regardless of any such courtesy reminder(s).

As part of this annual process, Vendors are required to access the Portal (refer to Section 4.9 [Access to the Portal](#)) to submit the AOV to PCI SSC and confirm, in part, that:

- Changes have been applied to the Listed and Validated KMO Service in a way that is consistent with the *KMO Standard* and Program Requirements;
- The Listed and Validated KMO Service continues to meet the requirements of the *KMO Standard* and Program Requirements;

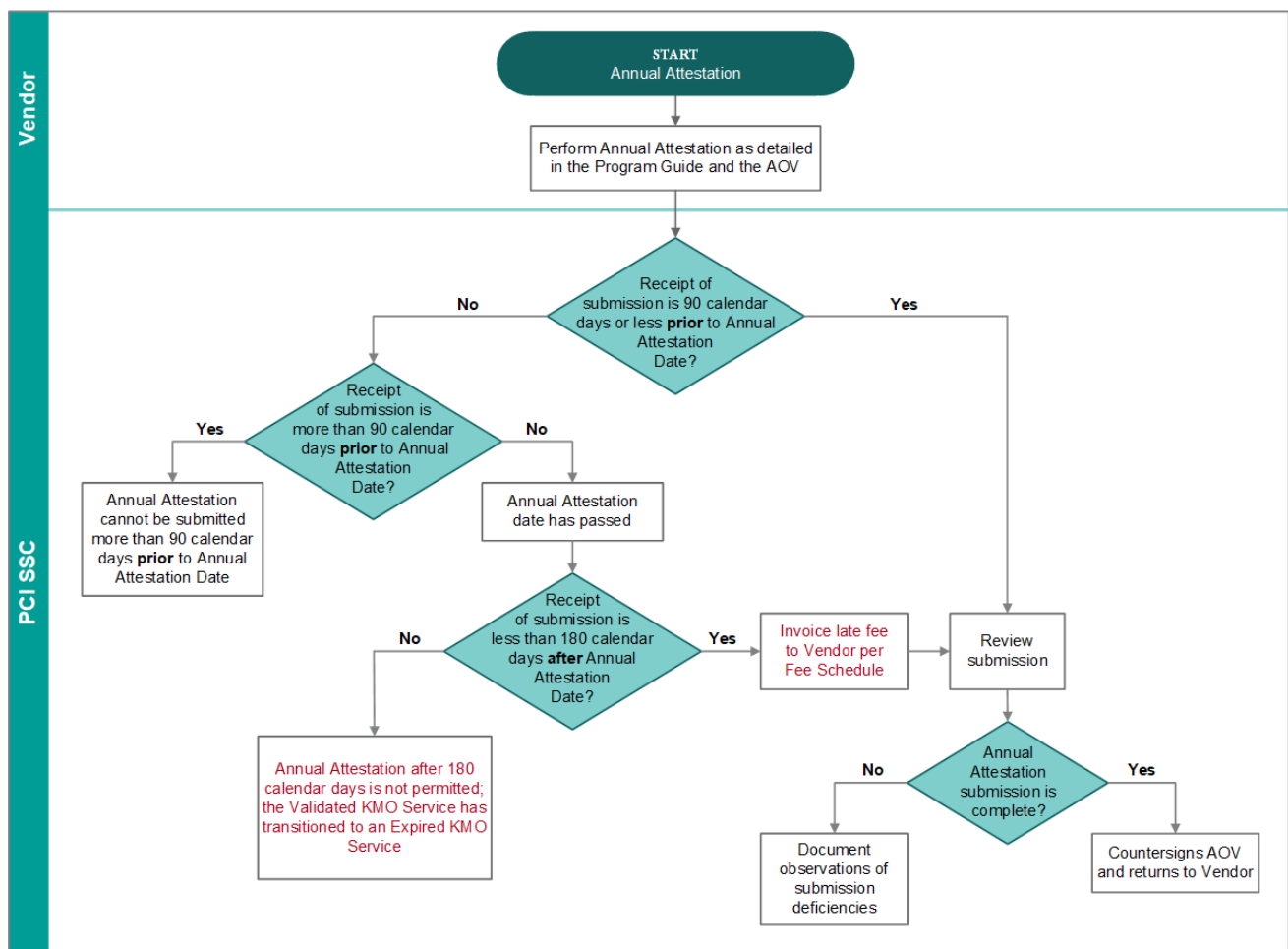
Note: The Vendor is required to consider the impact of external threats and whether updates to the Listed KMO Service are necessary to address changes to the external threat environment.

PCI SSC will, following receipt of the updated AOV:

1. Review the submission for completeness; and
2. If completeness is established, sign and return a copy of the updated AOV to the Vendor.

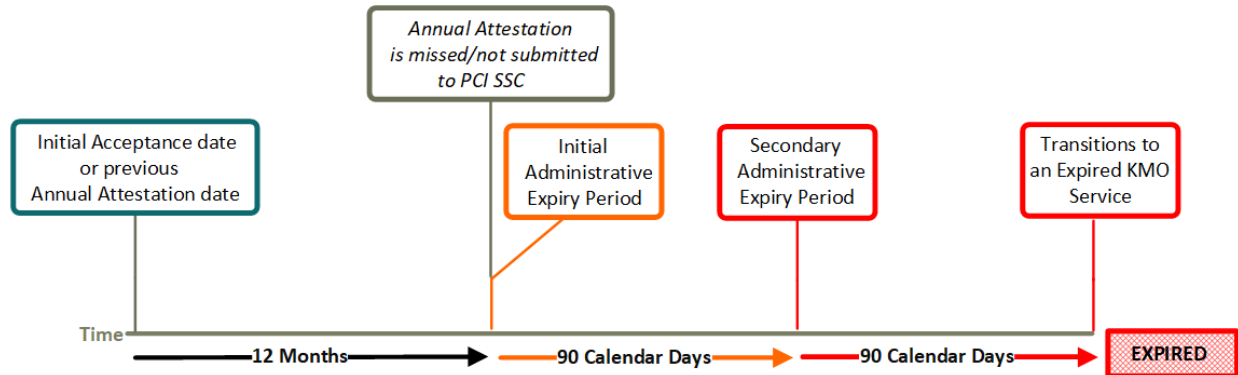
The following diagram provides a general overview of the Annual Attestation process:

Figure 4: Annual Attestation Process



If an AOV is not submitted and Accepted by PCI SSC on or before the Listed and Validated KMO Service's current Annual Attestation date, the respective Listing will be subject to Administrative Expiry, as follows:

Figure 5: Administrative Expiry



6.1.1 Initial Administrative Expiry Period

The corresponding KMO Service Listing will be updated to show the KMO Service's Annual Attestation date in **Orange** for a period up to 90 consecutive calendar days unless the Annual Attestation requirements of the Program are satisfied.

If the updated and complete AOV is received by PCI SSC within this initial 90-day period, PCI SSC will, upon Acceptance, remove the **Orange** status from the KMO Service Listing.

6.1.2 Secondary Administrative Expiry Period

If the updated and complete AOV is not received and Accepted by PCI SSC within the 90-day initial Administrative Expiry period, the corresponding KMO Service Listing will be updated to show the KMO Service's Annual Attestation date in **Red** for a period up to 90 consecutive calendar days.

Once a Listed KMO Service is in this secondary Administrative Expiry period (**Red**), a Full Assessment (including applicable Program fees) is required to relist the KMO Service and avoid Expiry.

If a Full Assessment is conducted, submitted to, and Accepted by PCI SSC before the KMO Service Expires, the submission will qualify as a Reassessment as described herein. Otherwise, once Expired, any Full Assessment submission of the KMO Service to PCI SSC will be considered a New Assessment.

6.1.3 Administrative Expiry

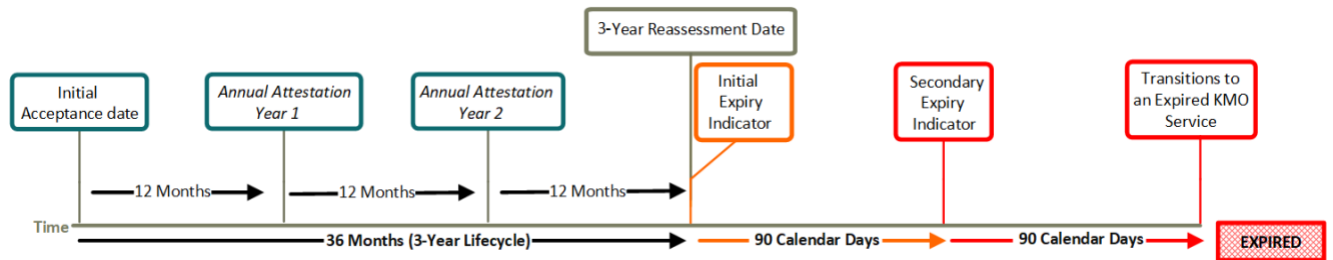
If a KMO Service's Listing has been in a **Red** status for more than 90 consecutive calendar days (over 180 days overdue in satisfying the Annual Attestation requirements of the Program), it becomes an Expired KMO Service and is no longer considered a Validated KMO Service.

6.2 Reassessment Process

A Listed and Validated KMO Service is eligible for Reassessment provided all applicable Program Requirements have been satisfied. A Reassessment is a Full Assessment of a Listed and Validated KMO Service that is submitted to and Accepted by PCI SSC at the end of the 3-year lifecycle, before it is redesignated as an Expired KMO Service. A Reassessment may benefit from defined Program allowances that a New Assessment cannot.

As a Listed and Validated KMO Service approaches its 3-year Listing Reassessment date, PCI SSC will provide a courtesy notification to the Vendor of the pending Listing Expiration. However, it is the sole responsibility of the Vendor to initiate a Reassessment of their Validated KMO Service regardless of any such courtesy reminder(s). The Vendor can choose to perform a Reassessment; otherwise, the Validated KMO Service will be redesignated as an Expired KMO Service, which is no longer considered to be a Validated KMO Service, Accepted, or Listed.

Figure 6: Reassessment Timeline and Listing Expiry



6.2.1 Listing Expiry

A Listed KMO Service, for which a new Acceptance based on a Full Assessment has not occurred on or before the Listed KMO Service's applicable Reassessment date, will immediately appear in **Orange** for up to 90 consecutive calendar days and in **Red** thereafter for up to 90 additional consecutive calendar days.

If a new Acceptance has not occurred within 180 consecutive calendar days following the Listed KMO Service's applicable Reassessment date, it will be redesignated as being an Expired KMO Service, which is no longer considered a Validated KMO Service, Accepted, or Listed. Any assessment of an Expired KMO Service is considered a New Assessment.

7 Program Fees

Program Fees are denoted in the PCI SSC Programs Fee Schedule on the Website. Program fees are non-refundable and are subject to change upon posting of revised fees.

PCI SSC will invoice the Vendor for all associated Program fees for a submission, and the Vendor is required to pay these fees directly to PCI SSC.

Program fees must be received by PCI SSC for a submission to be reviewed and Accepted (provided the submission satisfies the *KMO Standard* and Program Requirements).

If the AOV is not received by PCI SSC on or before the respective Annual Vendor Attestation date, there is a Program 'late' fee associated with the processing of AOVs received as part of the Annual Attestation process for a Listed and Validated KMO Service.

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

8 Security Issue Notification

In the event of a Security Issue (as defined in the *VRA*) relating to a Listed and Validated KMO Service, the *VRA* requires the KMO Vendor to notify PCI SSC and comply with various other requirements. Vendors must be aware of and adhere to all their obligations under the *VRA* in the event of a Security Issue, including but not limited to the following:

8.1 Notification and Timing

Notwithstanding any other legal obligations, pursuant to the *VRA*, Vendors are required to notify PCI SSC of all such Security Issues within the period of time specified in the *VRA*, including the related information pursuant to the *VRA*, and to provide follow-up information which may include (without limitation) an assessment of any impact (possible or actual) that the Security Issue has had, may have, or will have.

8.2 Notification Format

The Vendor's Security Issue notification to PCI SSC must be in writing in accordance with the *VRA* and should be preceded by an e-mail to the PCI SSC KMO Program Manager at kmo@pcisecuritystandards.org.

8.3 Notification Details

Information provided pursuant to such written notice and to the PCI SSC KMO Program Manager should include (but is not limited to) the following:

- The name, PCI SSC approval (Reference) number, and any other relevant identifiers of each of the Vendor's Product(s) affected by the Security Issue;
- A description of the general nature of the Security Issue;
- The Vendor's good-faith assessment of its knowledge at the time as to the scope and severity of the vulnerability or vulnerabilities associated with the Security Issue (using CVSS or other industry-accepted standard scoring); and
- Assurance that the Vendor is following its Vulnerability Handling Policies.

8.4 Actions following a Security Breach or Compromise

In the event of PCI SSC being made aware of a Security Issue related to a Listed and Validated KMO Service, PCI SSC may take the actions specified in the *VRA* and additionally, may:

- Notify Participating Payment Brands that a Security Issue has occurred.
- Request a copy of the latest version of the Vendor's Vulnerability Handling Policies.
- Communicate with the Vendor about the Security Issue and, where possible and permitted, share information relating to the Security Issue.
- Support the Vendor's efforts to mitigate or prevent further Security Issues.
- Support the Vendor's efforts to correct any Security Issues.
- Work with the Vendor to communicate and cooperate with appropriate law enforcement agencies to help mitigate or prevent further Security Issues.

8.5 Withdrawal of Acceptance

PCI SSC reserves the right to refuse, suspend, withdraw, revoke, cancel or place conditions upon its Acceptance of (and accordingly, remove from the List of Validated KMO Services) any KMO Service in accordance with the *VRA*, including but not limited to, if the applicable KMO Service or Vendor fails to satisfy applicable Program Requirements or PCI SSC reasonably determines that (a) the KMO Service does not provide sufficient protection against current threats and conform to the requirements of the KMO Program, (b) the continued Acceptance of the KMO Service represents a significant and imminent security threat to its users, or (c) such action is necessary in light of a related Security Issue or to ensure compliance with applicable law.

Appendix A KMO Services and Acceptance

Acceptance of a given KMO Service by PCI SSC only applies to the specific KMO Service validated by a KMO Assessor Company qualified to assess the specific KMO Service, and subsequently Accepted by PCI SSC (the “Accepted Product”). If any aspect of a KMO Service is different from that which was validated by the KMO Assessor Company qualified to assess the specific KMO Service, and Accepted by PCI SSC – even if the different KMO Service (the “Alternate Product”) conforms to the basic product description of the Accepted KMO Service – the Alternate Product should not be considered Accepted by PCI SSC, nor promoted as Accepted by PCI SSC.

No KMO Vendor or other third party may refer to a KMO Service 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 KMO Vendor or its KMO Service, 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 KMO Service 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 KMO Vendor or the functionality, quality, or performance of the Validated KMO Service 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 KMO Services

B.1 KMO Vendor Company Name

The Vendor of the Validated KMO Service. May include a hyperlink to the company's website at the Vendor's discretion.

B.2 Location(s)

The physical location(s) as designated by the KMO Vendor for the KMO Service.

B.3 Validated KMO Service Name

The name is provided by the Vendor and is the name by which the Validated KMO Service is known. The name cannot contain any variable or special characters.

Note: Use of PCI SSC's name, standards, program names and/or associated acronyms (e.g., PCI DSS, SLC, KMO, PTS, etc.) in Listing names are strictly prohibited. PCI SSC reserves the right to reject any submission that violates this naming policy.

B.4 Listing Reference Number

PCI SSC assigns the unique Reference Number upon Acceptance of the Validated KMO Service as a result of a Full Assessment;

Notes: A Listed and Validated KMO Service that undergoes a Reassessment to the same major version of the KMO Standard that is subsequently Accepted and Listed will retain its existing Reference Number.

A Listed and Validated KMO Service that undergoes a Reassessment to a new major version of the KMO Standard that is subsequently Accepted and Listed will result in an updated (new) Reference Number.

All New Assessments of KMO Services will result in a newly assigned Reference Number.

B.5 KMO Service Type

Denotes the defined KMO Service type that was assessed and validated. For eligible KMO Service types, refer to Section [1.3 KMO Services](#).

B.6 KMO KIF Service Function(s) Provided

This field contains additional context by which the KMO Service was assessed/evaluated. Refer to Section [1.3.1 KMO Service](#).

B.7 Cryptography Supported

Denotes the cryptography supported by the KMO Service, per key data type. The options are provided below. A Listing must include at least one type of classical cryptography for any key data type supported. A Listing may optionally support more than one cryptography type for each key data type.

Classical

- Symmetric (TDES)
- Symmetric (AES)
- Asymmetric (RSA/ECC)

PQC

- Asymmetric (PQC)

B.8 Key Injection Supported

Denotes the type of key injection supported for each key data type supported (e.g., PIN keys, P2PE keys, etc.), which can be:

- **Not Applicable:** Key injection is not an applicable function for this KMO Service.
- **Local Key Injection:** Local key injection in a KIF is supported (indicated per key data type).
- **Remote Key Injection:** Remote key injection is supported (indicated per key data type).

B.9 Key Data Types Supported

Denotes the type of keys supported by the KMO Service, e.g., PIN, P2PE, etc. The explicit list of key data types is located in the *ROV Template* and are determined as part of the KMO Assessment. At least one key data type must be supported.

B.10 Other KMO Service Dependencies

Denotes Other Listed KMO Services being relied on.

Notes: *Certain KMO Services can outsource to other predefined KMO Services. Refer to Section 3.5 Listed KMO Service Outsourcing Matrix.*

New Assessments and Reassessments of KMO Services will not be Accepted if they use other Expired KMO Services. Refer to Section 3.6.2 Expired KMO Services.

Expired KMO Service dependencies will be denoted as being Expired in the details of the parent Listed KMO Service. Refer to Section 3.6.3 Listed KMO Services with Expired Dependencies.

While a KMO Service may include third-party services (including those offering services potentially eligible for being Listed as a Validated KMO Service), those third-party services are not identified within the KMO Service's Listing or on the List of Validated KMO Services. Any such use of a third-party service in another KMO Service would require either its own independent Listing as a KMO Service, if eligible, or an assessment as part of each KMO Service of which the third-party service is a part of.

B.11 KMO Standard Version

The version of the *Payment Card Industry (PCI) Key Management and Operations (KMO)™ Standard (KMO Standard)* used to validate the KMO Service.

B.12 KMO Service Status

Denotes the status of the KMO Service, which is either Validated or Expired.

Upon Acceptance based on a Full Assessment, the status of the Validated KMO Service on being Listed is denoted as Validated.

If the relevant Program Requirements are not satisfied as described herein, the status on the Listing will be denoted as Expired, resulting in the Validated KMO Service transitioning to being an Expired KMO Service.

Note: *Each Payment Brand maintains and enforces its own compliance programs, including but not limited to requirements, mandates, and/or dates for use, fines or penalties, or other requirements as it may pertain to KMO Services. Questions regarding how the use of services denoted on the Website as Expired may affect compliance obligations should be addressed to the merchant's acquirer and/or the relevant Payment Brands.*

B.13 KMO Assessor Company

The KMO Assessor Company is the company that performed the assessment and validation, and determined that the KMO Service is in accordance with the *KMO Standard* and Program Requirements.

B.14 Annual Vendor Attestation Date

The Annual Vendor Attestation Date is the date by which the Vendor must satisfy the Annual Vendor Attestation (Annual Attestation) process, which occurs at the 12- and 24-month mark from the last date of Acceptance based on a Full Assessment.

B.15 Reassessment Date

The Reassessment Date is the 3-year date from the last date of Acceptance based on a Full Assessment by which time the Vendor can choose to undergo and [re]submit the KMO Service for another Full Assessment to the *KMO Standard* and Program Requirements to, provided Acceptance occurs, maintain their Listing. If the Validated KMO Service has not transitioned to being an Expired KMO Service, then it is eligible for a Reassessment; otherwise it must undergo a New Assessment.

B.16 Notes

Listings may contain additional informative notes to provide context to the Listing.