Payment Card Industry (PCI)
Qualified PIN Assessor (QPA)

Program Guide

Version 1.2

For use with PIN Security Requirements v3.x

May 2025

Document Changes

Date	Version	Description
January 2019	1.0	This is the first release of the *PCI QPA Program Guide.*
September 2021	1.1	Removed requirement that QPAs must submit CPEs to PCI SSC Clarified requirement for QPAs to have appropriate skills for assessments Added requirement that QPAs must be trained on the version of the standard they are assessing Added guidance regarding remote assessments Added Appendix B to provide additional QA guidance Performed minor clarifications in language throughout
May 2025	1.2	Moved [previous] Terminology (Section 2) and Related Publications (Section 3) to Sections i and ii, respectively Updated or added the following to support PIN Service listings on the Website: – Several terms and definitions in the Terminology section – Roles and Responsibilities (Section 3) – Term “Customers” changed to “PIN Service Providers” (Section 3.4) – [new] Section 4.3.2, PIN Service Provider Portal – [new] Sections 5.4 - 5.6 Removed portions of [previous] Sections 6 (now Section 4, QPA Qualification Process) and [previous] Section 8 (QPA Quality Management Program) to reduce redundancy with duplicate content in the *QPA Qualification Requirements* Minor wording updates for clarification and consistency with other PCI SSC Programs

Contents

i Terminology

For purposes of this Program Guide, the following terms are defined as set forth in *Table 1* or in the current version of the corresponding PCI SSC documents referenced in *Section ii*, unless otherwise indicated. All such documents are available on the Website.

Table 1: Glossary of Terms

Term	Definition / Source / Document Reference
Accepted, Acceptance	Refer to definitions in VRA (for QPA Company submissions) and PSPRA (for direct Service Provider submissions)
Good Standing	Refer to the QPA Agreement
List of PCI PIN Service Providers	The authoritative list of PCI PIN Service Providers appearing on the Website
Listing	The information regarding a PIN Service Provider appearing on the applicable PIN Listing after Acceptance has occurred
Participating Payment Brand	Refer to the QPA Agreement.
PCI PIN Assessment	Refer to the *QPA Qualification Requirements*.
PCI SSC	Acronym for "Payment Card Industry Security Standards Council."
PIN Service Provider (or "Service Provider")	An entity whose PIN services have been assessed and validated as satisfying the requirements of the *PCI PIN Standard*. PIN Service Providers may, but are not required, to have their assessed and validated PIN service listed on the List of PCI PIN Service Providers. See *Section 5.4*.
PIN Service Provider Release Agreement (or "PSPRA")	The then-current version of (or successor document to) the Payment Card Industry PIN Service Provider Release Agreement on the form then approved by PCI SSC for PIN Service Providers choosing to self-submit requests to have their PIN Service listed on the List of PCI PIN Service Providers, as from time to time amended and made available on the Website
Portal	PCI SSC's secure web portal for the QPA Program
Primary Contact	Refer to the QPA Agreement
QPA	Acronym for "Qualified PIN Assessor"
QPA Agreement	The then-current version of (or successor document to) the *Qualified PIN Assessor Agreement* attached as Appendix A to the *PCI PIN Assessor Qualification Requirements*
QPA Company	A company that has been qualified, and continues to be qualified, by PCI SSC to perform PCI PIN Assessments
QPA Employee	An employee of a QPA Company who has been qualified, and continues to be qualified, by PCI SSC to perform PCI PIN Assessments

Term	Definition / Source / Document Reference
QPA List	The then-current list of QPA Companies published by PCI SSC on the Website
QPA Program Manager	The PCI SSC point of contact for QPA Program related matters, e-mail: pcipin@pcisecuritystandards.org.
QPA Program	Refer to *QPA Qualification Requirements*.
QPA Qualification Requirements	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Qualification Requirements for Qualified PIN Assessors (QPA)*, as from time to time amended and made available on the Website
QPA Requirements	Refer to the *QPA Qualification Requirements*.
Vendor Release Agreement (or "VRA")	The then-current version of (or successor document to) the Payment Card Industry Vendor Release Agreement on the form then approved by PCI SSC for PIN Service Providers (and other Vendors) choosing to have their PIN Service listed on the List of PCI PIN Service Providers pursuant to a submission by a QPA Company, as from time to time amended and made available on the Website
Website	The then-current PCI SSC website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org

ii Related Publications

This document should be reviewed in conjunction with other relevant PCI SSC publications, including but not limited to current publicly available versions listed in *Table 2* and available on the Website.

Table 2: Related Publications

Document name	Description
Payment Card Industry PCI PIN Security Requirements and Testing Procedures (*PCI PIN Standard*)	The specific technical and operational security requirements and assessment procedures used by QPA Companies and QPA Employees to validate compliance with the *PCI PIN Standard*
PCI PIN Attestation of Compliance (PIN AOC)	The form for QPA Companies, QPA Employees, and PIN Service Providers to attest to the results of a PCI PIN Assessment, as documented in the *PIN Report on Compliance*
PCI Qualified PIN Assessor (QPA) Qualification Requirements	Defines the baseline set of requirements that must be met by a QPA Company and QPA Employees to perform their respective roles in connection with PCI PIN Assessments
PCI PIN Template for Report on Compliance (PIN ROC)	Provides detail on how to document the findings of a PCI PIN Assessment and includes the mandatory template for use in completing a Report on Compliance
PCI SSC Programs Fee Schedule	Available on the Website, lists the current fees for specific qualifications, tests, retests, training, and other services
PCI SSC Remote Assessment Guidelines and Procedures	Detailed guidelines and procedures for performing PCI SSC Assessments remotely
QPA Feedback Form	Provides the PIN Service Provider an opportunity to offer feedback regarding the QPA and the PCI PIN Assessment process https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_PIN_assessors_feedback
PIN Service Provider Release Agreement (PSPRA)	Available to PIN Service Providers in the Portal, the PSPRA establishes the terms and conditions under which PIN submissions made directly by PIN Service Providers are Accepted and included on the PCI PIN Services List.
Vendor Release Agreement (VRA)	Available on the Website, the VRA establishes the terms and conditions under which PIN submissions made by QPA Companies are Accepted and included on the PCI PIN Services List.

1 Introduction

This Program Guide provides information to Qualified PIN Assessor (QPA) Companies and QPA Employees pertinent to their roles in connection with the PCI SSC Qualified PIN Assessor (QPA) program. The QPA Program is further described in *QPA Qualification Requirements* on the Website. Companies wishing to apply for QPA Company status should first consult the *QPA Qualification Requirements*. Capitalized terms used, but not otherwise defined herein, have the meanings set forth in *Section i*, or in the *QPA Qualification Requirements*, as applicable.

2 Updates to Documents and Security Requirements

This Program Guide is expected to change as necessary to align with updates to the *PCI PIN Standard* and other PCI SSC Standards. Additionally, PCI SSC provides interim updates to the PCI community through a variety of means, including required QPA Employee training, e-mail bulletins and newsletters, frequently asked questions, and other communication methods.

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

3 Roles and Responsibilities

There are several stakeholders in the QPA Program. The following sections define their respective roles and responsibilities.

3.1 Participating Payment Brands

In relation to the *PCI PIN Standard*, 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:

Note: *Contact details for the Participating Payment Brands can be found in FAQ #1142 on the Website.*

- Managing compliance enforcement programs (requirements, mandates or dates for compliance validation).
- Establishing penalties and fees.
- Establishing validation process requirements and who must validate.
- Endorsing qualification criteria.
- Responding to PIN or key-related compromises.

3.2 PCI Security Standards Council

PCI SSC is the standards body that maintains the PCI SSC Standards and supports programs and documentation. In relation to the QPA Program, PCI SSC:

***Note**: PCI SSC does not assess entities for PCI PIN Security compliance.*

- Maintains the PCI SSC Standards and related testing requirements, programs, and supporting documentation.
- Provides training for and qualifies QPA Companies and QPA Employees to perform PCI PIN Assessments.
- Lists QPA Companies and QPA Employees on the Website.
- Maintains the List of PCI PIN Service Providers on the Website.
- Maintains an Assessor Quality Management (AQM) program.
- Assesses QPA Company compliance with PCI SSC's quality levels and qualification requirements. See the *QPA Qualification Requirements* for additional information.

3.3 Qualified PIN Assessor Companies (QPA Companies)

A QPA Company is an organization that has been qualified as a QPA Company by PCI SSC, has been added to the QPA List and, through its QPA Employees, is thereby authorized to validate adherence to the *PCI PIN Standard* in accordance with applicable QPA Program requirements for QPA Program purposes. Prior to being added to the QPA List, the QPA Company's QPA Employees must successfully complete all applicable QPA Program training requirements. Active QPA Companies and QPA Employees can be found through a search tool on the PCI SSC Website.

***Note:** While the Primary Contact's role includes helping facilitate and coordinate with PCI SSC regarding administrative or technical questions, Primary Contacts as well as QPA Companies and QPA Employees are strongly encouraged to check the FAQs published on the Website prior to contacting PCI SSC with questions.*

The "Primary Contact" (defined in the QPA Agreement) at the QPA Company is the liaison between PCI SSC and the QPA Company. See *Section 4.2* for additional details.

QPA Companies and their QPA Employees' responsibilities in connection with the QPA Program include, but are not limited to, the following:

- Adhering to the *QPA Qualification Requirements* and this *QPA Program Guide*.
- Maintaining knowledge of and ensuring adherence to current and relevant PCI PIN guidance and instructions located in the Document Library section of the Website.
- Performing PCI PIN Assessments in accordance with the *PCI PIN Standard*, including but not limited to:
  - Selecting employees, systems, and system components that accurately represent the assessed environment if sampling is employed.
  - Providing an opinion about whether the assessed entity meets PCI PIN Security Requirements.
  - Effectively using the *PCI PIN Reporting Template* to produce PIN ROC
  - Validating and attesting as to an entity's PCI PIN Security compliance status.
  - Maintaining documents, workpapers, and interview notes that were collected during the PCI PIN Assessment and used to validate the findings.

  - Applying and maintaining independent judgment in all PCI PIN Assessment decisions.
  - Conducting follow-up assessments, as needed.
  - Stating assessed entity compliance with *PCI PIN Standard*. PCI SSC does not approve PIN ROCs from a technical perspective, but performs QA reviews on PIN ROCs to ensure that the documentation of testing procedures performed is sufficient to support the results of the PCI PIN Assessment. See the *QPA Qualification Requirements* for additional information. See *Appendix B, Eight Guiding Principles Validated by Four Criteria (Four Cs)*, to understand PCI SSC's baseline for assessor quality.
- Submitting the PIN AOC to PCI SSC signed by both the QPA and PIN Service Provider, if applicable.

3.4 PIN Service Providers

The role of a PIN Service Provider (also referred to as candidate PIN Service Provider) in connection with the QPA Program includes the following:

- Understanding compliance and validation requirements of the current *PCI PIN Standard*.
- Maintaining compliance with the *PCI PIN Standard*.
- Complying with terms of the Vendor Release Agreement or *PIN Service Provider Release Agreement*, as applicable, including the adoption and implementation of Vulnerability Handling Policies (further described in the VRA and PSPRA) consistent with industry best practices.
- Selecting a QPA Company (from the QPA List) to conduct their PCI PIN Assessment, as applicable.
- Providing sufficient documentation to the QPA Employee to support the PCI PIN Assessment.
- Remediating any issues of non-compliance as required.
- Submitting required compliance materials to Participating Payment Brands, Networks, and Acquiring Entities as directed.
- Providing feedback on QPA Employee performance in accordance with the *QPA Feedback Form* on the Website.
- Notifying Participating Payment Brands if they suspect or discover a PIN or key-related data breach.
- Optionally, and if applicable (for PIN Service Providers choosing to be included on the List of PCI PIN Service Providers) submitting the PIN AOC to PCI SSC, signed by both the QPA and PIN Service Provider.

4 QPA Qualification Process

To help ensure that each QPA Company and QPA Employee possesses the requisite knowledge, skills, experience, and capacity to perform PCI PIN Assessments in a proficient manner and in accordance with industry expectations, each company and individual desiring to perform PCI PIN Assessments must be qualified by PCI SSC as a QPA Company or QPA Employee (as applicable), and then must maintain that qualification in Good Standing. Details on the QPA qualification process including initial qualification, requalification, timeframes, fees and other details are described in the PCI Qualified PIN Assessor (QPA) Qualification Requirements document available on the Website.

4.1 Subcontracting

A QPA Company's engagement, hiring, or other use of any other company, organization, or individual (other than an QPA Employee directly employed by that QPA Company) to perform any aspect of the services to be performed in connection with any PCI PIN Assessment is considered to be subcontracting and requires prior written consent by PCI SSC in each instance. This applies regardless of whether the subcontracted entity or individual is already a QPA Company or a QPA Employee of a different QPA Company.

The QPA Company must also provide PCI SSC proof of bound insurance coverage for all such subcontractors to demonstrate policies are in accordance with QPA Program insurance coverage requirements (see Appendix B of the *QPA Qualification Requirements*).

PCI SSC's consent to any such subcontracting shall be subject to such terms, conditions, and requirements as PCI SSC may in its sole discretion deem necessary, reasonable, or appropriate under the circumstances.

Note: *To obtain PCI SSC's consent to the use of a given subcontractor, please contact the QPA Program Manager at pcipin@pcisecuritystandards.org.*

4.2 Primary Contact

The QPA Company must designate a Primary Contact to act as communication liaison to PCI SSC. The Primary Contact has sole authorization to submit requests to PCI SSC related to the QPA Program. PCI SSC must be notified immediately in writing if there is a change in the Primary Contact. The Primary Contact is not required to be a QPA Employee.

Notices from PCI SSC to the Primary Contact may be communicated via the Portal, e-mail, registered mail, or any other method permitted by the QPA Agreement.

It is the responsibility of the Primary Contact to respond to PCI SCC in a timely manner.

4.3 Portal

The Portal is PCI SSC's secure web portal for the QPA Program; correspondence with QPAs and PIN Service Providers (e.g., all PIN AOC submissions) typically occur via the Portal.

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

4.3.1 Assessor Portal

Access to the Portal is granted once the candidate QPA Company is qualified as a QPA Company. QPA Employees receive logon instructions upon passing the QPA training exam, and PCI SSC enters their grades into the database. Primary Contacts receive higher-level access than employees. Access is granted to the Primary Contact upon e-mail request to the QPA Program Manager. Additional credentials can be requested by the QPA's Primary Contact through the PCI SSC PIN Program Manager.

For QPAs, the Portal includes the following:

- Editable versions of the PIN reporting templates (PIN ROC and PIN AOC)
- Library of published PCI SSC Assessor Newsletters
- Recorded webinars
- QPA certificates in PDF format
- Primary Contact name, e-mail, and address
- Individual certifications – i.e., CISSP, CISA, etc. – entry page with expiration date, if applicable
- View PIN AOC submissions submitted by the QPA Company, and PIN AOC submissions submitted by PIN Service Providers for which the QPA Company performed the Assessment

Along with the items noted above, the QPA Primary Contact has access to:

- Requalification training approval page for all QPA Employees
- Insurance policies with respective expiration dates
- Complete list of all QPA Employees and their requalification dates
- Addresses for all QPA training locations throughout the year

QPA Employees should check the Portal on a regular basis for new information and updates.

4.3.2 PIN Service Provider Portal ("Vendor Portal")

Access to the Portal requires the PIN Service Provider's Primary Contact to first register through a link on the Website – this can be found under the *Product & Solutions* tab, *PIN Service Providers* menu item. The PIN Service Provider Primary Contact will receive logon instructions upon review and confirmation by PCI SSC.

4.4 FAQs and Guidance Documents

QPA Employees should refer to the Frequently Asked Questions (FAQ) section of the PCI SSC Website to obtain further guidance on questions relating to PCI PIN Assessments. It is the responsibility of each QPA Employee to monitor the Website on a regular basis as information is updated frequently. RSS feed updates are available for the PCI Standards document library on the Website.

QPA Employees should periodically familiarize themselves with all Information Supplements and guidance published to the Website.

Note: *Additional FAQs may also be found in the Frequently Asked Questions Category for each Standard in the Document Library on the Website.*

Questions submitted through the FAQ tool will only be accepted if submitted by the Primary Contact.

5 PCI PIN Assessment Process

To demonstrate compliance with the *PCI PIN Standard*, PIN Service Providers may be required to have periodic PCI PIN Assessments conducted as required by each Participating Payment Brand.

Note: *PIN Service Providers should consult with their network, acquirer, or Participating Payment Brands about their requirement for a PCI PIN Assessment.*

PCI PIN Assessments are required to be conducted by a QPA Company through its QPA Employees, if applicable, in accordance with the *PCI PIN Standard*, which contains requirements, testing procedures, and guidance to ensure that the intent of each requirement is understood. Each QPA Employee must work only on those PCI SSC Assessments for which the QPA Employee is qualified by PCI SSC, has appropriate skills, including technology and language, and has an appropriate understanding of the PIN Service Provider's business.

The QPA Employee will document the results of the PCI PIN Assessment in the PIN ROC, including which portions of the PCI PIN Assessment were conducted onsite. The ROC must accurately represent the assessed environment, and the security controls tested and validated by the QPA Employee.

5.1 Security Incident Response

The QPA Company must have a documented process for notifying the applicable PIN Service Provider when the QPA Company or an employee thereof, during any QPA Program related services, becomes aware of an actual or suspected breach of PIN or key-related data within that PIN Service Provider's environment. The process must include instructions for notifying the PIN Service Provider in writing of the incident and related findings and informing the PIN Service Provider of its obligations to notify the Participating Payment Brands in accordance with each Participating Payment Brand's notification requirements. The notification must be retained in accordance with the QPA Company's evidence-retention policy along with a summary of the incident and what actions were taken.

5.2 Remote Assessments

While onsite PCI PIN Assessments are expected, the use of remote PCI PIN Assessment methods may be a suitable alternative in scenarios where an onsite PCI PIN Assessment is not feasible. In such cases, refer to the PCI SSC Remote Assessment Guidelines and Procedures (available on the Website) for guidance.

5.3 Documenting a PCI PIN Assessment

For each PCI PIN Assessment, the resulting PIN ROC must use the most current PIN ROC Reporting Template available on the Portal. The PIN ROC must be accompanied by a PIN Attestation of Compliance (PIN AOC), available in the Documents Library on the Website. A duly authorized officer of the QPA Company must sign the PIN AOC, which summarizes whether the PIN Service Provider meets the requirements of the *PCI PIN Standard*, and any related findings.

The intent of requiring a signature from a "duly authorized officer" is to ensure that the QPA Company is aware of and has formally signed off on the work performed and, accordingly, recognizes its obligations and responsibilities in connection with that work. Although the signatory's job title need not include the term "officer," the signatory must be formally authorized by the QPA Company to sign such documents on the QPA Company's behalf and should be competent and knowledgeable regarding the QPA Program and related requirements and duties.

By signing the PIN AOC, the PIN Service Provider is attesting that the information provided in the PIN AOC and accompanying *PIN Report on Compliance* is true and accurate. The date on the PIN AOC cannot predate the date on the PIN ROC.

The PIN AOC is submitted to the requesting entity/entities according to applicable submission requirements.

5.4 List of PCI PIN Service Providers

5.4.1 Submissions for PIN Service Listing

Once the PIN ROC and PIN AOC are complete, if the PIN Service Provider wishes to be listed on the List of PCI PIN Service Providers, there are two options:

1. The QPA may submit the completed PIN AOC to PCI SSC via the Portal, along with the PIN Service Provider-signed VRA (unless PCI SSC already has a copy of the current version of the VRA as available on the Website executed and on file from the PIN Service Provider); or
2. The PIN Service Provider may submit the PIN AOC to PCI SSC via the Portal (see *Section 4.3.2*) and accept the PIN Service Provider Release Agreement in the Portal when prompted.

5.4.2 PIN Service Provider Acceptance and Listing

Upon receiving a submission per *Section 5.4.1*, PCI SSC issues an invoice to the PIN Service Provider for the applicable fee (see *Section 5.6*). After the PIN Service Provider has paid the invoice, PCI SSC reviews the PIN AOC, typically within 30 calendar days of payment of invoice.

If the submission is complete and meets all applicable requirements (as documented in the QPA Program Guide and related program materials), PCI SSC will sign and return a copy of the PIN AOC to both the PIN Service Provider and the QPA Company via the Portal, and add the PIN Service Provider details to the List of PCI PIN Service Providers. PIN Service Listings are valid for 2 years from the signature date of the QPA Acknowledgement in Part 3c of the PIN AOC.

Note: *There must be consistency between the information in materials submitted via the Portal, and the "Details" fields within the Portal. Incomplete or inconsistent submissions may result in a significant delay in the processing of requests for listing and/or may not be Accepted by PCI SSC.*

5.4.3 Listing Information

Each Listing on the List of PCI PIN Service Providers contains the following information at a minimum:

- Company (PIN Service Provider)
- *PCI PIN Standard* Version
- Expiry Date
- Validated by (QPA Company)
- Reference #

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

5.4.4 Expired Listings

When the expiry date of a Listing has passed, the Listing Expiry Date shall appear in orange bold text for up to 90 calendar days. When the expiry date of a Listing has passed 90 calendar days the date shall appear in red bold text to indicate the Listing was not revalidated prior to its expiry.

Note: *PIN Service Providers should consider timing submissions to PCI SSC as close to completion of the relevant PCI PIN Assessment as possible in order to maximize the duration of their Listing, as the Listing will show as Expired on the Website* ***2 years after the date of the QPA Acknowledgement and signature in Part 3c of the PIN AOC****; PCI SSC will not prorate the invoice to account for past-dated AOCs.*

5.5 Release Agreements

Among other things, the VRA and PSPRA (each referred to as a "Release Agreement" and each available on the Website) cover confidentiality issues, the PIN Service Provider's agreement to PCI PIN Program requirements, policies and procedures, and give permission to the PIN Service Provider's QPA to release PIN AOCs (and related materials, as applicable) to PCI SSC for review. Release Agreements also require PIN Service Providers to adopt and comply with industry standard Vulnerability Handling Policies.

For each PCI PIN Assessment in which the PIN Service Provider wishes to have their QPA submit the AOC for Listing on the List of PCI PIN Service Providers, along with any required documents and materials, the PIN Service Provider must submit to the QPA a copy of the PIN Service Provider's signed Vendor Release Agreement on the then-current VRA form. The VRA must be delivered directly to PCI SSC by the QPA, along with the corresponding PIN AOC. Where the PIN Service Provider chooses to perform its own PIN AOC submission to the Portal, the PIN Service Provider agrees to the terms of the PSPRA in the Portal.

Note: *Submissions to PCI SSC received directly from the PIN Service Provider require the PIN Service Provider to acknowledge and accept the terms of the PSPRA via a web-based form in the Portal.*

PCI SSC will not review any submission or update thereto without the then-current, signed or accepted, correct type of Release Agreement (based on method of submission) on file for the respective PIN Service Provider.

Where a VRA is required, so long as an executed current VRA is on file with PCI SSC for the relevant PIN Service Provider, it is not required to re-submit the same version of the VRA with each subsequent PIN AOC for the same PIN Service Provider.

5.6 PCI PIN Listing Fees

Each PIN Service Provider wishing its PIN Service to be listed on the List of PIN Service Providers must pay a Listing fee for each Listing. Fees are invoiced to the PIN Service Provider by PCI SSC and must be paid to PCI SSC according to the instructions accompanying the invoice before the PIN submission will be processed. Upon Acceptance, PCI SSC will sign and return a copy of the PIN Attestation of Compliance (AOC) to both the PIN Service Provider and the QPA Company that performed the PCI PIN Assessment.

Note: *The PIN Service Provider pays all PCI PIN Assessment-related fees directly to the QPA Company (these fees are negotiated between the PIN Service Provider and the QPA Company).*

There are no annual recurring PCI SSC fees associated with the Acceptance of a PCI PIN Listing submission. Refer to the Programs Fee Schedule on the Website for more information. Program fees are non-refundable and are subject to change upon posting of revised fees on the Website.

5.7 PCI PIN Assessment Evidence Retention

As per Section 4.5 “Evidence (Assessment Workpaper) Retention” of the *QPA Qualification Requirements*, QPA Companies must gather evidence to support the contents of each PIN ROC. The QPA Company must secure and maintain, for a minimum of three (3) years from the PIN ROC completion date, digital and/or hard copies of case logs, audit results, workpapers, e-mails, interview notes, and any technical information – e.g., screenshots, configuration settings – that were created and/or obtained during the PCI PIN Assessment. This information must be available upon request by PCI SSC and its affiliates. The QPA Company must also provide a copy of the evidence-retention policy and procedures to PCI SSC upon request.

For additional details on what the QPA Company’s Evidence Retention Policy must include, see Section 4.5 of the *QPA Qualification Requirements* document, available on the Website.

6 General Guidance

6.1 Resourcing / Transfers

QPA Employee status may transfer to another company as the QPA Employee changes employers. The following should be noted when a QPA Employee moves to a new company:

1. If the new company is not an active QPA Company, the QPA Employee's qualification will be inactive until employed by an active QPA Company. Inactive status does not suspend or modify requalification deadlines. A QPA Employee cannot requalify while their employer is not an active QPA Company.
2. If the QPA Employee moves to an active QPA Company and is to be utilized by that QPA Company as a QPA Employee, the Primary Contact of the new QPA Company must notify the QPA Program Manager of the transfer. The QPA Employee must be listed under the new company on the PCI Website prior to participating in any PCI PIN Assessment. The following information must be provided to the QPA Program Manager:
   - Name
   - E-mail
   - Phone
   - Notification if the QPA Employee is acting as a sub-contractor.

6.2 PCI SSC Logos and Marks

Unless expressly authorized, a QPA Company or QPA Employee is not permitted to use any PCI SSC trademark, service mark, certification mark, or logo without the prior written consent of PCI SSC in each instance. A QPA Program-specific logo is available on request via e-mail to the QPA Program Manager.

Note: *PCI SSC does not issue an official PCI seal, mark, or logo that companies are permitted to use when they achieve PCI PIN compliance. The PCI Security Standards Council logo is a registered trademark and may not be used without authorization. You may not use or encourage or enable others to use the phrases or marks: PCI Compliant, PCI Certified, PCI PIN Compliant, PCI PIN Certified, or PCI with a check mark, or any other mark or logo that states or implies compliance or conformance with any of the PCI SSC Standards.*

6.3 QPA Company Changes

In the event that a QPA Company requires an alias or a trade name be added to its listing on the Website – for example, "trading as" or Doing Business As (DBA) scenarios – please contact the QPA Program Manager for the *Assessor Name Change Request Form*.

Appendix A Quality Criteria for QPA Audits

As part of AQM's monitoring of quality within the QPA Program, AQM performs holistic QPA Audits of QPA Companies against the following general criteria:

- QPA Company documentation (per the *QPA Qualification Requirements*)
- Workpapers/Evidence Retention
- Ethics
- Reporting

Examples of documents/evidence AQM may seek to validate the above criteria are as follows:

QPA Company Documentation (per the QPA Qualification Requirements)	
1	QPA Company's QA Manual includes an accurate QA process flow, identification of QA manual process owner, and evidence of annual review by the QA manual process owner.
2	QPA Company's QA Manual includes a requirement for all QPA Employees to regularly monitor the Website for updates, guidance, and new publications relating to the QPA Program.
3	QPA Company's Code of Conduct Policy supports – and does not contradict – the PCI SSC Code of Professional Responsibility.
4	QPA Company's Security and Incident Response Policy is consistent with PCI SSC guidance and is appropriately available within the QPA Company.
Workpapers/Evidence Retention	
1	QPA Company's Evidence Retention Policy includes all required content defined within the *QPA Qualification Requirements*. For example, it includes formal assignment of an employee responsible for ensuring the continued accuracy of the Workpaper Retention Policy.
2	Relevant evidence is provided by QPA Company for all tests that are required to be performed.
3	QPA Company was able to provide a blank copy of the QPA Company's Workpaper Retention Policy, as well as produce copies signed by the QPA Employee(s).
Ethics	
1	QPA Company and QPA Employees fulfilled the objective of providing an independent, unbiased representation of the facts of the case, including no significant or intentional omissions or misrepresentations of facts.
2	QPA Company and QPA Employees maintained independence throughout the engagement and provided adequate reporting as to how this was validated and maintained.

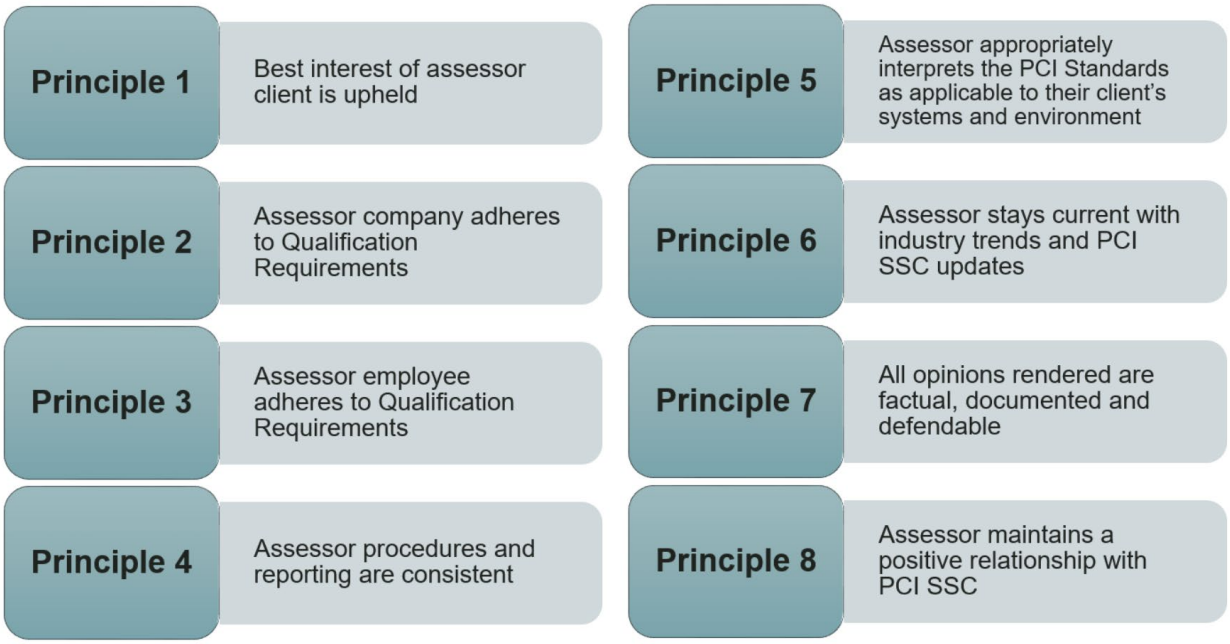
Reporting	
1	QPA Company and QPA Employees used the appropriate templates for reports.
2	QPA Company and QPA Employees provided clear, consistent detail as to how requirements were validated to be in place, avoiding excessive use of cut and paste.
3	QPA Company and QPA Employees provided a compensating control worksheet for each compensating control noted within the ROC reporting.
4	For the high-level diagram, QPA Company and QPA Employees addressed all Reporting Instructions, including identification of connected entities.
5	QPA Company and QPA Employees provided a thorough response that includes details of testing and observation to validate the integrity of the segmentation mechanisms within the Summary Overview.
6	When explaining how the QPA Company and QPA Employees evaluated that the scope was accurate and appropriate, QPA Company and QPA Employees included sufficient detail to demonstrate the findings that validated the scope (rather than just the method used).
7	QPA Company and QPA Employee responses go beyond repeating the verbiage within the Reporting Template and include substantive and relevant detail as to how the testing procedure was in place.

Appendix B Eight Guiding Principles Validated by Four Criteria (Four Cs)

The Eight Guiding Principles represent a quality baseline for PCI SSC assessor companies and individuals (each an "Assessor"), and can be validated by four criteria: consistency, credibility, competency, and conscientiousness - or "the Four Cs."

Figure 1 shows the Eight Guiding Principles.

Figure 1: Eight Guiding Principles



PCI SSC reviews Assessor work product and stakeholder feedback with the expectation that the Assessor:

- Has followed the requirements of the applicable PCI SSC Program as documented in applicable Program documentation (for example, Qualification Requirements, Program Guides, agreements, etc.), and
- Has acted in the best interests of the PIN Service Provider in an ethical manner that results in factual, documented, and defendable opinions.

Program participants must keep up with PCI SSC updates (including but not limited to updates to the *QPA Qualification Requirements* and *QPA Program Guide*, monthly PCI SSC Assessor Newsletter articles, published FAQs on the Website, and content from relevant PCI SSC webinars).

The Four Cs are useful measurements to evaluate the strength and quality of the Assessor's approach and/or conclusions and can help the Assessor ensure that work can be defended in a meaningful way.