Security Standards Council®

Payment Card Industry (PCI)
Qualified PIN Assessors

Program Guide
Version 1.0

January 2019

Document Changes

Date	Version	Description
January 2019	1.0	This is the first release of the *PCI QPA Program Guide.*

Contents

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 4 below, or in the *QPA Qualification Requirements*, as applicable.

2 Related Publications

This document should be reviewed in conjunction with other relevant PCI SSC publications, including but not limited to current publicly available versions of the following, each available on the Website.

Document name	Description
Payment Card Industry PCI PIN Security Requirements and Testing Procedures (PCI PIN Standard)	Lists the specific technical and operational security requirements and provides the assessment procedures used by assessors to validate PCI PIN compliance.
PCI SSC Programs Fee Schedule	Lists the current fees for specific qualifications, tests, retests, training, and other services.
PCI PIN Attestation of Compliance (PIN AOC)	A form for Customers to attest to the results of a PCI PIN Assessment, as documented in the *PIN Report on Compliance*
PCI Qualification Requirements for Qualified PIN Assessors (QPAs)	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.
QPA Feedback Form	Gives the Customer 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

3 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.

4 Terminology

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

Term	Definition / Source / Document Reference
Customer	See Section 5.4 below
Good Standing	Refer to QPA Agreement
Primary Contact	Refer to QPA Agreement.
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
QPA Requirements	Refer to QPA Qualification Requirements.
QPA List	The then-current list of QPA Companies published by PCI SSC on the Website.
QPA PM	QPA Program Manager contact by e-mail: QPA@pcisecuritystandards.org.
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.
Participating Payment Brand	Refer to definition in QPA Agreement.
PCI PIN Assessment	Refer to QPA Qualification Requirements.
PCI SSC	Payment Card Industry Security Standards Council, which manages the PCI SSC Standards.
Remediation	See Section 8.3 below.
Website	The then-current PCI SSC website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org.

5 Roles and Responsibilities

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

5.1 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:

- 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.

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

5.2 PCI Security Standards Council

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

- 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 an Assessor Quality Management (AQM) program.

As part of the quality assurance (QA) process, PCI SSC assesses whether overall QPA Company operations appear to conform to PCI SSC's quality levels and qualification requirements. See Section 8 titled "Assessor Quality Management" for additional information.

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

5.3 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.

The "Primary Contact" (defined in the QPA Agreement) at the QPA Company is the liaison between PCI SSC and the QPA Company.

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 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, facilities, systems, and system components accurately representing the assessed environment if sampling is employed.
  - Being on-site at assessed entity during the PCI PIN Assessment.
  - Providing an opinion about whether the assessed entity meets PCI PIN Security Requirements.
  - Effectively using the *PCI PIN Reporting Template* to produce *PCI PIN Reports on Compliance*. (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 whether or not the assessed entity has achieved 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 Section 8, "Assessor Quality Management," for additional information.

***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.*

5.4 Customers

The role of PCI PIN Assessment customers (service providers, financial institutions, etc.—collectively, “Customers”) 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 at all times.
- 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.

6 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.

In order to achieve qualification as a QPA Company, the candidate company and at least one of its employees must satisfy all QPA Requirements (defined in the QPA Qualification Requirements) applicable to QPA Companies and QPA Employees. All such QPA Companies are then identified on the QPA List on the Website, and all such QPA Employees are added to the Website's search tool.

Only those QPA Companies and QPA Employees qualified by PCI SSC and included in the QPA List or Website search tool (as applicable) are recognized by PCI SSC to perform PCI PIN Assessments.

6.1 Requalification

All QPA Companies must be requalified by PCI SSC on an annual basis. The annual QPA Company requalification date is based upon the QPA Company's *original qualification date.* QPA Company requalification requires payment of annual training and QPA Company fees, as well as continued compliance with applicable QPA Requirements.

Each QPA Employee must be requalified by PCI SSC on an annual basis. The annual requalification date is based upon the QPA Employee's *previous qualification date*. QPA Employee requalification requires successful completion of requalification training and payment of annual training fees.

For example, a one-year requalification for a certification with a current qualification date of 15 November 2018 will be changed to 15 November 2019 upon successful completion regardless of whether the requalification was completed on 31 October 2018 or 25 November 2018.

***Note:** Negative feedback from Customers, PCI SSC, Participating Payment Brands, or others may impact the QPA Company's and/or QPA Employee's eligibility for requalification.*

6.1.1 Requalification Timeframe

To ensure adequate time to complete requalification requirements, QPA Employees should note:

- Registration for requalification training must be completed (and approved, where applicable) prior to the QPA Employee's qualification expiration date. A candidate who is not registered prior to that expiry date must re-enroll as a new candidate.
- A two-week grace period is provided beyond the candidate's expiry date in order to complete requalification training; however, candidates will not be qualified by PCI SSC during this time and will not be requalified until the requalification exam is successfully completed.
- Access to the course and requalification exam will be granted only after payment is processed, and candidates will have access to the exam at most four weeks prior and two weeks past their expiration date.

- If a candidate is enrolled for requalification training and fails to take the training within the defined period, payment will be forfeited in full and the individual will need to reapply as a new QPA Employee candidate.

6.2 Fees

Each QPA Company must pay an annual QPA Company Fee in order to become and remain qualified as a QPA Company. All QPA Company Fees and QPA training fees are specified on the Website in the *PCI SSC Programs Fee Schedule* and are subject to change.

All fees must be paid in US dollars (USD) by check, by credit card, or by wire transfer to the PCI SSC bank account specified for such purpose on the lower half of the invoice.

The option for credit card payment is not offered on QPA Company fee invoices. However, the option can be added to the invoice upon request. A fee of 3% of the total invoice will be added for processing.

6.2.1 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 to 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 QPA@pcisecuritystandards.org.*

6.2.2 Insurance

The QPA Company must adhere to all requirements for insurance coverage required by PCI SSC, as outlined in Appendix B, “Insurance Coverage,” of the QPA Qualification Requirements.

Prior to qualification as a QPA Company and annually thereafter, the QPA Company is required to provide a certificate to PCI SSC from each insurance company as evidence that all required insurance is in force for each region with respect to which it operates. The certificates must state the applicable policy numbers, dates of expiration, and limits of liability.

Insurance must cover the following (or otherwise be acceptable to PCI SSC):

- Worker’s compensation
- Employer’s Liability (with a limit of $1,000,000)

- Commercial General Liability Insurance ($1,000,000 minimum, $2,000,000 annual aggregate) including:
  - Products
  - Completed Operations
  - Advertising Injury
  - Personal Injury
  - Contractual Liability Insurance
- Commercial Automobile Insurance ($1,000,000 minimum limit)
- Crime/Fidelity Bond, both first and third party ($1,000,000 minimum for each loss and annual aggregate)
- Technology Errors and Omissions, Cyber-Risk, and Privacy Liability Insurance ($2,000,000 minimum for each loss and annual aggregate)

6.3 QPA Continuing Professional Education (CPE)

To remain in Good Standing, all QPA Employees must provide proof of information systems security training within the last 12 months of the requalification date in accordance with the current version of the *PCI SSC CPE Maintenance Guide*.

A QPA employee must also earn a minimum of 20 CPE credits per year and a minimum of 120 CPE credits per rolling three-year period.

6.4 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. The 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 designated 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.

6.5 Assessor Portal

Access to the Portal is granted once the QPA Company is qualified as a QPA Company. QPA Employees receive log-on instructions upon passing the QPA training exam, and PCI SSC enters their grades into the database. Primary Contacts receive a higher-level access than employees. Access is granted to the Primary Contact upon e-mail request to the QPA Program Manager.

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

The Portal includes the following information:

- Editable version of the PIN ROC Reporting Template
- Library of published Assessor Newsletters
- Recorded Webinars
- QPA Certificates in PDF format

- Primary Contact name, e-mail, and address
- Individual Certification—i.e., CISSP, CISA, etc.—entry page with expiration date, if applicable

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

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

Check the Portal on a regular basis for new information and updates.

6.6 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. The Website should be monitored on a weekly basis as information is updated. RSS feed updates are available for the PCI Standards document library.

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

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

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

7 PCI PIN Assessment Process

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

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.

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

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

7.1 Security Incident Response

The QPA Company must have a documented process for notifying the applicable Customer 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 Customer's environment. The process must include instructions for notifying the Customer in writing of the incident and related findings and informing the Customer 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.

7.2 Documenting a PCI PIN Assessment

For each PCI PIN Assessment, the resulting PIN Report on Compliance (PIN ROC) must follow the most current PIN ROC Reporting Template available on the Website. The PIN ROC must be accompanied by an 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 entity that was assessed is in compliance with 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 being done 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 assessed entity 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 ROC.

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

7.3 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.

If a Customer refuses to provide the QPA Company with the documentary evidence—for example, because it contains information that is sensitive or confidential to the Customer—the QPA Company and the Customer should work together to ensure that the evidence is retained securely at the Customer site and as required by the QPA Qualification Requirements, including being made available upon request by PCI SSC for a minimum of three (3) years from the date of PIN ROC completion. It is recommended that the QPA Company and the Customer have a formal agreement that outlines each party’s responsibilities in this matter, which agreement must be consistent with and comply with the disclosure requirements specified in the QPA Agreement.

Even if the actual, documented evidence is to be retained by the Customer, the QPA Company must keep records to identify the specific evidence that was used during the PCI PIN Assessment—for example, digital and/or hard copies of the documents or testing results that are being retained by the Customer. The QPA Company’s records should clearly identify which pieces of evidence were used for each requirement, how the evidence was validated, and the findings that resulted from each piece of evidence. The QPA Company should retain enough Information to ensure that the complete, actual evidence used during the PCI PIN Assessment can be identified for retrieval if needed; for example, in the event of an investigation or if a finding needs to be reviewed.

As part of the PCI SSC’s Assessor Quality Management (“AQM”) QPA Program audit process (“QPA Audit”) and in other AQM quality assurance (“QA”) review work as needed, it is common for AQM to request both the QPA Company’s Workpaper Retention Policy and a sample of PCI PIN Assessment workpapers. This is to ensure the QPA Company has a current documented, implemented Workpaper Retention process consistent with the requirements defined in the QPA Qualification Requirements—including appropriate level of detailed instructions for QPA Employees to comply with. AQM may additionally request blank and/or executed copies of the QPA Company’s Workpaper Retention Policy agreement that each QPA Employee is required to sign, and may request additional evidence to demonstrate that all Assessment Results and Related Materials (defined in the QPA Agreement) relating to the PCI PIN Assessments for the sampled ROC were in fact retained in accordance with the procedures defined in the Workpaper Retention Policy prior to releasing the final PIN ROC for that PCI PIN Assessment.

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

8 QPA Quality Management Program

The QPA Company must have implemented an internal quality assurance program as documented in its Quality Assurance Manual. Assessor Quality Management (AQM) at PCI SSC performs periodic QPA Company audits, which are a holistic review of the QPA Company's internal documentation required by the QPA Qualification Requirements. Such QPA Company audits include review of PIN ROCs to provide reasonable assurance that a baseline standard of quality has been achieved in the documentation of testing procedures performed. Refer to Appendix A to understand sample criteria against which QPA Companies are measured during QPA Audits.

A QPA Audit by the PCI SSC AQM team will result in a finding of:

- **Satisfactory –** A notification letter will be sent with specific opportunities for improvement listed. Mandatory call with AQM team to discuss.

  A "Satisfactory" finding indicates that the audit findings reasonably confirmed (1) the QPA Company/Employee's ongoing adherence to the current QPA Qualification Requirements; (2) that the QPA Company's quality policy documentation is implemented and maintained according to the QPA Qualification Requirements; and (3) the QPA Company/Employee's ongoing general adherence to reporting requirements as evidenced by sampled PIN ROCs.

- **Needs Improvement –** A notification letter will be sent with specific opportunities for improvement listed. Mandatory call with AQM team to discuss.

  A "Needs Improvement" finding indicates that there were minor findings and/or opportunities for improvement identified that assessors should address to ensure continued adherence with program documentation. Still, the audit findings reasonably confirmed (1) the QPA Company/Employee's ongoing adherence to the current QPA Qualification Requirements; (2) that the QPA Company's quality policy documentation is implemented and maintained according to the QPA Qualification Requirements; and (3) the QPA Company/Employee's ongoing general adherence to reporting requirements as evidenced by sampled PIN ROCs.

- **Unsatisfactory –** A notification letter is sent with specific opportunities for improvement. Mandatory call with AQM team to discuss Remediation.

  An "Unsatisfactory" finding indicates that there were serious findings identified during the QPA Audit, including possible Violations to the QPA Agreement. This finding will result in Remediation and/or Revocation, per the current QPA Qualification Requirements. Audit findings that result in an Unsatisfactory finding mean that AQM could not confirm one or more of the following: (1) the QPA Company/Employee's ongoing adherence to the current QPA Qualification Requirements; (2) that the QPA Company's quality policy documentation is implemented and maintained according to the QPA Qualification Requirements; and (3) the QPA Company/Employee's ongoing general adherence to reporting requirements as evidenced by sampled PIN ROCs.

For further details on the Assessor Quality Management Program, please see the *QPA Qualification Requirements* document available on the Website.

8.1 Ethics

The QPA Company must adhere to professional and business ethics, perform its duties with objectivity, and limit sources of influence that might compromise its independent judgment in performing PCI PIN Assessments.

PCI SSC has adopted a *PCI SSC Code of Professional Responsibility* (the "Code," available on the Website) to help ensure that PCI SSC-qualified companies and individuals adhere to high standards of ethical and professional conduct. All PCI SSC-qualified companies and individuals must advocate, adhere to, and support the Code.

QPA Companies and QPA Employees are prohibited from performing PCI PIN Assessments of entities that they control or are controlled by, and entities with which they are under common control or in which they hold any investment.

> ***Note:*** *QPA Employees are permitted to be employed by only one QPA Company at any given time.*

QPA Companies and QPA Employees must not enter into any contract that guarantees a compliant PIN ROC.

QPA Companies must fully disclose in the PIN Report on Compliance if they assess Customers who use any security-related devices or security-related applications that have been developed or manufactured by the QPA Company, or to which the QPA Company owns the rights, or that the QPA Company has configured or manages.

Each QPA Company agrees that when it (or any QPA Employee thereof) recommends remediation actions that include one of its own solutions or products, the QPA Company will also recommend other market options that exist.

Each QPA Company must adhere to all independence requirements as established by PCI SSC. For a complete list, please see Section 2.2 in the *QPA Qualification Requirements.*

8.2 Feedback Process

At the start of each PCI PIN Assessment, the QPA Company must direct the Customer to the *QPA Feedback Form* on the Website and request that the Customer submit the completed form to PCI SSC through the PCI SSC website following the PCI PIN Assessment.

Any Participating Payment Brand, acquiring bank, or other person or entity may submit *QPA Feedback Forms* to PCI SSC to provide feedback on a PCI PIN Assessment, QPA Company, or QPA Employee.

Link to Feedback Form:
https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_PIN_assessors_feedback

8.3 Remediation Process

QPA Companies that do not meet all applicable quality assurance standards set by PCI SSC may be offered the option to participate in PCI SSC's QPA Company Quality Remediation program ("Remediation"). PCI SSC may offer Remediation in connection with any quality assurance audit, any violation (as defined in the QPA Qualification Requirements), or any other PCI SSC Program-related quality concerns, including but not limited to unsatisfactory feedback from Customers or Participating Payment Brands. The Remediation process includes:

- Remediation overview call and signed Remediation Agreement.
- Remediation Period of at least 120 days.
- QPA Company listing on the QPA List updated to "red" to notify merchants/service providers.
- An AQM case manager assigned to the QPA Company to offer support as it works to bring its quality level to the expected baseline standard of quality.
- The expectation of strong commitment from the QPA Company to achieve successful completion.
- Fees for review of work.

8.4 Revocation Process

A QPA Company (or any QPA Employee thereof) may be subject to revocation of its PCI SSC qualification ("Revocation") if found to be in breach of the Agreement or other QPA Requirements, including without limitation, for any of the following:

- Failure to perform PCI PIN Assessments in accordance with the PCI PIN Standard.
- Violation of any provision regarding non-disclosure of confidential materials.
- Failure to maintain at least one certified QPA Employee on staff.
- Failure to maintain physical, electronic, and procedural safeguards to protect the confidential and sensitive information.
- Unprofessional or unethical business conduct.
- Failure to successfully complete any required PCI SSC training.
- Cheating on any PCI SSC training exam.

Upon notification of pending QPA Company Revocation by PCI SSC, the QPA Company, or QPA Employee will have 30 days in which to appeal the ruling in writing to PCI SSC.

Revocation will result in removal of the QPA Company or QPA Employee from the QPA List or search engine, as applicable.

In the event of QPA Company Revocation, the QPA Company must immediately cease all advertising of its QPA Company qualification. It must also immediately cease soliciting for and performing all pending and active QPA Assessments unless otherwise instructed by PCI SSC and comply with the post-Revocation requirements specified in the QPA Agreement.

Refer to the QPA Qualification Requirements for details on the Revocation process.

9 General Guidance

9.1 Resourcing /Transfers

QPA Employees may transfer to another company. 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 its 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 should be supplied to the QPA Program Manager:
   - Name
   - E-mail
   - Phone
   - Notification if the QPA Employee is acting as a sub-contractor.

9.2 PCI SSC Logo

Unless expressly authorized, a QPA Company or QPA Employee cannot 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.

9.3 QPA Company Changes

In the event that a QPA Company requires an alias or a trade name 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.