Payment Card Industry (PCI)

QSA Program Guide

For Qualified Security Assessors (QSA)

Version 3.0

March 2021

Document Changes

Date	Version	Description
November 2016	1.0	First release of the QSA Program Guide
December 2017	2.0	• Added Associate QSA Program • Added Appendix A and B to provide sample criteria that QSA Companies are measured against during QSA Audits
March 2021	3.0	• Added requirement for QSA Annual QA Questionnaire • Added Appendices C and D to provide additional QA guidance • Clarified requirement for QSAs to have appropriate skills for assessments • Added requirement that QSAs must be trained on the version of the standard they are assessing • Added ability for QSAs to opt into PCI ISA Program • Removed requirement that QSAs must submit CPEs to PCI SSC • Performed minor clarifications in language throughout

Table of Contents

1 Introduction

This Program Guide provides information to QSA Companies and Assessor-Employees pertinent to their roles in connection with the PCI SSC Qualified Security Assessor (QSA) program (the "Program"). The Program is further described in *QSA Qualification Requirements* on the Website. Companies wishing to apply for QSA Company status should first consult the *QSA Qualification Requirements*. Capitalized terms used, but not otherwise defined herein, have the meanings set forth in *Section 1.3*, or in the *QSA Qualification Requirements*, as applicable.

1.1 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
CPE Maintenance Guide	Provides the number of CPEs required on an annual basis by assessors to remain certified.
Mentor Manual Template	A set of sample documents provided by PCI SSC for use by a QSA Company in creating and maintaining the *Mentor Manual* required for the Associate QSA Program. This template is available on the Website and in the Portal.
Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures ("PCI DSS")	Lists the specific technical and operational security requirements and provides the assessment procedures used by assessors to validate PCI DSS compliance.
PCI DSS Glossary of Terms, Abbreviations, and Acronyms (the "Glossary")	Lists and defines the specific terminology used in the PCI DSS.
PCI SSC Programs Fee Schedule	Lists the current fees for specific qualifications, tests, retests, training, and other services.
PCI DSS Qualification Requirements for Qualified Security Assessors (QSAs)	Defines the baseline set of requirements that must be met by a QSA Company and Assessor-Employees in order to perform their respective roles in connection with PCI DSS Assessments.
PCI DSS Template for Report on Compliance ("ROC Reporting Template")	Provides detail on how to document the findings of a PCI DSS Assessment and includes the mandatory template for use in completing a *Report on Compliance*.
PCI SSC Information Supplements	Intended to provide additional guidance on specific topics, including recommendations and best practices. They are not intended to replace or supersede PCI SSC Standards, rather—as the name suggests—to supplement existing information.
QSA Feedback Form	Gives the Customer an opportunity to offer feedback regarding the QSA and the assessment process. https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors_feedback

1.2 Updates to Documents and Security Requirements

This Program Guide is expected to change as necessary to align with updates to the PCI DSS and other PCI SSC Standards. Additionally, PCI SSC provides interim updates to the PCI community through a variety of means, including required Assessor-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.

1.3 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. All such documents are available on the Website:

Term	Definition / Source / Document Reference
AOC	Acronym for Attestation of Compliance. Refer to the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* (Glossary) for details.
Assessor-Employee	QSA Employee or Associate QSA Employee, as applicable. Refer to *QSA Qualification Requirements* for details.
Assessor Portal (Portal)	Web-based application made available to PCI SSC qualified assessors to access PCI SSC program documentation and forms.
Associate QSA Employee (AQSA)	Refer to *QSA Qualification Requirements*.
Associate QSA Program (AQSA Program)	The component of the Program dedicated to enabling QSA Companies to develop new resources into fully qualified QSA Employees, as further described herein and in the *QSA Qualification Requirements*.
CDE	Acronym for Cardholder Data Environment. Refer to the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* (Glossary).
CPE	Acronym for Continuing Professional Education.
Good Standing	Refer to *QSA Qualification Requirements*.
Mentor	Refer to *QSA Qualification Requirements*
Mentor Manual	The documentation required to be maintained by a QSA Company as part of its participation in the Associate QSA Program.
PA-DSS	Acronym for Payment Application Data Security Standard. Refer to the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* (Glossary).
Primary Contact	Refer to QSA Agreement.

Term	Definition / Source / Document Reference
QSA Agreement	Appendix A of *QSA Qualification Requirements*.
QSA Company	Refer to *QSA Qualification Requirements*.
QSA Employee	Refer to *QSA Qualification Requirements.*
QSA Requirements	Refer to *QSA Qualification Requirements.*
QSA List	The then-current list of QSA Companies published by PCI SSC on the Website.
QSA PM	QSA Program Manager contact e-mail *qsa@pcisecuritystandards.org*.
QSA Qualification Requirements	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Qualification Requirements for Qualified Security Assessors (QSA)*, as from time to time amended and made available on the Website.
QSA Services	Refer to the QSA Agreement.
Payment Application	Refer to the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* (Glossary).
Participating Payment Brand	Refer to QSA Agreement.
PCI DSS Assessment	Refer to *QSA Qualification Requirements*.
PCI SSC	Acronym for PCI Security Standards Council, which manages the PCI SSC Standards.
PCI SSC Assessment	Refer to *QSA Qualification Requirements*.
PCI Standards	Refer to *QSA Qualification Requirements*.
Remediation	The correction of vulnerabilities identified within an information system.
ROC	Acronym for *Report on Compliance*. Refer to the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* (Glossary).
SAQ	Acronym for Self-Assessment Questionnaire. Refer to the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* (Glossary).
Security Issue	Refer to *QSA Qualification Requirements*.
Website	The then-current PCI SSC Website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org.

2 Roles and Responsibilities

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

2.1 Participating Payment Brands

In relation to the PCI DSS, 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.*

- Defining merchant and service provider levels
- Managing compliance enforcement programs (requirements, mandates or dates for compliance)
- Establishing penalties and fees
- Establishing validation process requirements and who must validate
- Approving and posting compliant entities, such as service providers
- Endorsing qualification criteria
- Responding to cardholder data compromises.

2.2 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 QSA Program, PCI SSC:

- Maintains the PCI SSC Standards and related validation requirements, programs and supporting documentation.
- Provides training for and qualifies QSA Companies and Assessor-Employees to perform PCI DSS Assessments.
- Lists QSA Companies on the Website.
- Maintains an Assessor Quality Management (AQM) program.

As part of the quality assurance (QA) process, PCI SSC assesses whether overall QSA Company operations appear to conform to PCI SSC's quality levels and qualification requirements. See *Section 5*, *Assessor Quality Management Program* for additional information.

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

2.3 Qualified Security Assessor Companies (QSA Companies)

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

The Primary Contact at the QSA Company is the liaison between PCI SSC and the QSA Company.

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

- Adhering to the *QSA Qualification Requirements* and this *Program Guide*.
- Maintaining knowledge of and ensuring adherence to current and relevant PCI DSS guidance and instructions located in the Document Library section of the Website.
- Ensuring that each QSA Employee works only on those PCI SSC Assessments for which the QSA Employee is properly qualified by PCI SSC, has appropriate skills (including technology and language), and has an appropriate understanding of the Customer's/Client's business.
- Performing PCI DSS Assessments in accordance with the PCI DSS, including but not limited to:
  - Validating and confirming Cardholder Data Environment (CDE) scope as defined by the assessed entity.
  - 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 DSS Assessment.
  - Evaluating compensating controls as applicable.
  - Providing an opinion about whether the assessed entity meets PCI DSS Requirements.
  - Effectively using the *PCI DSS ROC Reporting Template* to produce Reports on Compliance.
  - Validating and attesting as to an entity's PCI DSS compliance status.
  - Maintaining documents, workpapers, and interview notes that were collected during the PCI DSS Assessment and used to validate the findings.
  - Applying and maintaining independent judgement in all PCI DSS Assessment decisions.
  - Conducting follow-up assessments, as needed.
  - Stating whether or not the assessed entity has achieved compliance with PCI DSS. PCI SSC does not approve ROCs from a technical perspective, but performs QA reviews on ROCs to ensure that the documentation of testing procedures performed is sufficient to support the results of the PCI DSS Assessment. See *Section 5*, *Assessor Quality Management Program* for additional information.
- Refer to *Appendix C, Eight Guiding Principles Validated by Four Criteria (Four Cs)* to understand PCI SSC's baseline for assessor quality.

> ***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 QSA Companies and Assessor-Employees are strongly encouraged to check the FAQs published on the Website prior to contacting PCI SSC with questions.*

2.4 Customers

The role of PCI DSS Assessment customers (merchants, service providers, financial institutions, etc.—collectively, “Customers”) in connection with the Program includes the following:

- Understanding compliance and validation requirements of the current PCI DSS.
- Maintaining compliance with the PCI DSS at all times.
- Defining Cardholder Data Environment (CDE) scope per guidance provided in PCI DSS.
- Selecting a QSA Company (from the QSA List) to conduct their PCI DSS Assessment, as applicable.
- Providing sufficient documentation to the QSA to support the PCI DSS Assessment.
- Providing related attestation (e.g., proper scoping and network segmentation).
- Remediating any issues of non-compliance as required.
- Submitting the completed *Report on Compliance* or SAQ to their acquirer or Participating Payment Brands, as directed by the Participating Payment Brands.
- Providing feedback on QSA performance in accordance with the *QSA Feedback Form* on the Website.
- Notifying their acquirer and/or Participating Payment Brands if they suspect or discover a cardholder data breach.

3 Qualification Process

In an effort to help ensure that each QSA Company and Assessor-Employee possesses the requisite knowledge, skills, experience, and capacity to perform PCI DSS Assessments in a proficient manner and in accordance with industry expectations, each company and individual desiring to perform PCI DSS Assessments must be qualified by PCI SSC as a QSA Company or QSA Employee (as applicable), and then must maintain that qualification in Good Standing.

***Note:** The QSA certification is a requirement for other program certifications such as PA-DSS and P2PE.*

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

When a QSA Company has been active for at least two years, it is eligible to apply to join the Associate QSA Program and, accordingly, to apply to qualify eligible employees as Associate QSA Employees. For more information, see *Section 3.2*, *Associate QSA Program*.

QSA Employees are qualified to perform PCI SSC Assessments only to the version(s) of the PCI SSC Standard(s) for which they have successfully completed training.

Only those QSA Companies and QSA Employees qualified by PCI SSC and included on the QSA List or Website search tool (as applicable) are recognized by PCI SSC to perform PCI DSS Assessments. Associate QSA Employees may assist in performing PCI DSS Assessments as further described in this document.

3.1 Requalification

All QSA Companies must be requalified regionally by PCI SSC on an annual basis. The QSA Company's annual requalification date is based upon the QSA Company's original qualification date (on a per-region basis). QSA Company requalification requires payment of annual training and regional requalification fees (see the *PCI SSC Programs Fee Schedule* on the Website), as well as continued compliance with applicable QSA Requirements.

Each Assessor-Employee (QSA Employee and Associate QSA Employee, as applicable) must be requalified by PCI SSC on an annual basis. The annual requalification date is based upon the Assessor-Employee's previous qualification date. QSA Employee requalification requires proof of two active industry certificates. AQSA Employee requalification requires proof of applicable Continuing Professional Education (CPE). Both QSA Employee and AQSA Employee requalification requires payment of annual training fees and successful completion of training.

***Note:** Negative feedback from Customers (merchants, service providers, etc.), PCI SSC, Participating Payment Brands, or others may impact the QSA Company's and/or Assessor-Employee's eligibility for requalification.*

For example, a qualification date of 15 November 2020 will be updated to 15 November 2021 upon successful completion, regardless of whether the requalification was completed on 31 October 2020 or 25 November 2020.

3.1.1 Requalification Timeframe

To help ensure adequate time to complete requalification requirements, Assessor-Employees should note:

- Registration for requalification training must be completed (and approved, where applicable) prior to the Assessor-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 are not considered qualified by PCI SSC during this grace period and will not be requalified until they have successfully completed requalification training.
- Access to the requalification course and exam will be granted only after payment is processed, and candidates will have access to the exam up to four weeks prior to 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 QSA Employee (or AQSA, as applicable) candidate.

3.2 Associate QSA Program

The goal of the Associate QSA (AQSA) Program is to provide a path to enable QSA Companies to develop new resources to become QSA Employees through formal mentoring and monitoring skills development. Associate QSA Employees are qualified only by PCI SSC to support QSA Employees with PCI DSS Assessments. Refer to Section 3.3 of the *QSA Qualification Requirements* for more details on entry-level requirements for AQSAs.

Note: *Associate QSA Employees are qualified only by PCI SSC to support the performance of PCI DSS Assessments by QSA Employees.*

An Associate QSA Employee is able to apply to become a QSA Employee once they meet the QSA Requirements and have obtained the necessary Industry Certification(s) as stated in Section 3.2 of the *QSA Qualification Requirements*. It is not necessary for an Associate QSA Employee to retake the QSA Employee training and exam in the same year they qualify as a QSA Employee. There is no requirement regarding how long an individual must be an Associate QSA Employee before applying to become a QSA Employee. The QSA Company must inform the applicable Customer when an Associate QSA Employee has been assigned to work in connection with the PCI DSS Assessment of that Customer, and in which parts of the PCI DSS Assessment the Associate QSA Employee will be participating. The QSA Employee leading a PCI DSS Assessment (the "Lead QSA") and providing supervision to an Associate QSA Employee:

1. Is responsible for understanding the level of expertise of the Associate QSA Employee and their ability to perform any assigned part of the PCI DSS Assessment independently.
2. Is responsible to review all notes and/or evidence collected by the Associate QSA Employee.
3. Is responsible to make the actual compliance determination.

3.2.1 Associate QSA Duties

Each QSA Employee assisting on PCI DSS Assessments must be qualified by PCI SSC either as a QSA Employee or Associate QSA Employee. Duties of an Associate QSA Employee may include:

- Gathering of evidence (e.g., documentation and screenshots)
- Maintaining an inventory of documented evidence in adherence with the QSA Company's workpaper retention policy
- Documenting sections of the executive summary:
  - Detailing business descriptions
  - Identifying responsible people to be included in the ROC
  - Gathering list of third parties and lists of acquirers or connected entities
- Preparing draft sections of a ROC related to requirements for which the Associate QSA Employee has gathered the evidence
- Conducting interviews (under QSA Employee supervision), either directly or through a review of notes taken
- Reviewing documented evidence with specific criteria provided by a QSA Employee
- Following up on remediated findings with specific criteria provided by a QSA Employee
- Conducting data center/site visits with specific criteria provided by a QSA Employee (not intended for independent assessment of client's primary sites)

An Associate QSA Employee is *restricted* from performing the following duties:

- Leading a PCI DSS assessment
- Confirming PCI DSS compliance to Customers
- Signing Attestations of Compliance (AOCs)
- Validating the scope of a PCI DSS Assessment
- Selection of systems and systems components where sampling is used
- Evaluating compensating controls
- Evaluating customized controls
- Initiating or leading compliance discussions with payment brands or acquirers

3.3 Mentor Program

QSA Companies participating in the Associate QSA Program are required to implement and maintain a formal Mentor program to support development of the Associate QSA Employee's assessment skills and techniques and provide numerous opportunities for discussing growth and setting new objectives. The Mentor program must be documented in the QSA Company's *Mentor Manual*. The required *Mentor Manual Template* is available on the Website; and an editable version is available in the Portal and must be completed per the template's instructions. The QSA Company must provide a copy of its *Mentor Manual* to PCI SSC for review when applying to join the Associate QSA Program.

The Primary Contact for the QSA Company is ultimately responsible for providing oversight of the Mentor program to ensure the QSA Company's continued adherence to the QSA Requirements, including maintaining the *Mentor Manual* and performing associated audit activities. Any delegation of monitoring tasks assigned to the Primary Contact must be formally documented in the applicable section of the QSA Company's *Mentor Manual*.

Note: *If a Mentor withdraws from the QSA Company's Mentor program, affected Associate QSA Employees must be reassigned to another Mentor within 90 days. The QSA Company must notify the QSA Program Manager via e-mail if Associate QSA Employees cannot be reassigned within 90 days.*

The *Mentor Manual Template* content includes, but is not limited to, the following:

- QSA Company Mentor Program Overview
  - For recording QSAC-specific content such as contingency plan(s) for when mentors leave, and internal audit processes
  - To be completed/maintained by the Primary Contact or formal designee at least once every calendar year; and
  - Retained in the QSA Company *Mentor Manual*.
- AQSA-Mentor Assignment Log
  - For documenting assignments of eligible Mentor QSA Employees to Associate QSA Employees.
  - To be completed/maintained by the Primary Contact or formal designee at least once every 30 calendar days; and
  - Retained in the QSA Company *Mentor Manual*.
- Mentor Responsibilities Acknowledgment Form
  - To be signed by the Mentor before starting Mentor responsibilities and updated with the onboarding of each Associate QSA Employee.
  - To include acknowledgment of completion of Mentor training module; and
  - Retained in the QSA Company *Mentor Manual* within the AQSA-Mentor Assignment Log by Primary Contact or formal designee.
- AQSA Skills Summary Form
  - To be completed at onboarding with the Mentor and Associate QSA Employee and updated at least once every 90 calendar days to reflect the Associate QSA Employee's quarterly progress and
  - Retained by the Associate QSA Employee with a current copy provided to any Lead QSA with whom the Associate QSA Employee is working on a PCI DSS Assessment, to ensure the Lead QSA understands the level of expertise the Associate QSA Employee possesses.

- AQSA Engagement Summary
  - To be completed by the Lead QSA with whom the Associate QSA Employee is working on a PCI DSS Assessment.
  - To be used by the Lead QSA to acknowledge receipt and review of the most current AQSA Skills Summary Form and assign any tasks to the Associate QSA Employee. The Lead QSA must update the summary with feedback and/or opportunities for improvement and return the completed AQSA Engagement Summary to the Associate QSA Employee within 30 calendar days of the assigned tasks being completed.
  - To be retained (in copy) by the Lead QSA as part of the PCI DSS Assessment workpapers.
  - To be retained by the Associate QSA Employee for every PCI DSS Assessment for which the Associate QSA Employee completed tasks. Associate QSA Employee is responsible for providing the summary to the Mentor QSA at least once every 90 days for use when updating the AQSA Skills Summary Form.
- AQSA Development Tracking Log
  - For self-tracking PCI DSS Assessment work, learning opportunities, CPEs, etc.;
  - To be completed/maintained by the Associate QSA Employee at least once every 30 calendar days; and
  - Retained by the AQSA, who must provide executed log to the Mentor QSA for use when updating the AQSA Skills Summary Form at least once every 90 calendar days.

The Associate QSA Employee is ultimately responsible for ensuring the completion, retention and delivery to relevant parties of the *AQSA Skills Summary, AQSA Engagement Summary* and *AQSA Development Tracking Log*. The Lead QSA must maintain a copy of the completed *AQSA Engagement Summary* in the workpapers for each PCI DSS Assessment. If more than one AQSA is assisting on a PCI DSS Assessment, an *AQSA Engagement Summary* must be completed for each Associate QSA Employee. Similarly, the Lead QSA must complete an *AQSA Engagement Summary* for each separate PCI DSS Assessment if working with an Associate QSA Employee on multiple PCI DSS Assessments.

3.4 Assessor-Employee Continuing Professional Education (CPE)

QSA Employees who provide evidence of two active industry-recognized certifications (see *QSA Qualification Requirements* for details) at their requalification are not required to report CPEs to PCI SSC for the previous year.

An AQSA Employee must provide proof of information systems audit training within the last 12 months of their respective requalification date in accordance with the current version of the *CPE Maintenance Guide*.

3.5 Fees

Each QSA Company must pay an application processing fee and a regional qualification fee for each geographic region or country in which the QSA Company intends to perform PCI DSS Assessments. The application-processing fee is credited toward the initial regional qualification fee(s). All QSA Company fees are specified in the *PCI SSC Programs Fee Schedule* on the Website 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 regional 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.

3.5.1 Regions

- QSA Companies are authorized to perform PCI DSS Assessments and QSA-related duties only in the geographic region(s) or country(s) for which they have paid the regional or country fees, and as indicated on the QSA List.
- Under no circumstances may QSA Companies perform PCI DSS Assessments—or any QSA Services—outside of the qualified region(s) or country(ies).

  For example, if a Merchant is headquartered in the USA and has satellite offices in-scope for PCI DSS located in Singapore, the QSA Company must be qualified in both USA and Asia Pacific regions before they are permitted to perform QSA Services for the merchant.
- If QSA Services must be performed outside of the qualified region or country it may be necessary to engage a QSA Company qualified for that region or country to perform the related tasks. Refer to *3.5.2, Subcontracting*.
- To add or remove a region or country, contact the PCI SSC QSA Program Manager. Additional regions or countries will appear on the QSA List on the Website pending receipt of payment fees and evidence of insurance.

3.5.2 Subcontracting

A QSA Company's engagement, hiring, or other use of any other company, organization, or individual (other than an Assessor-Employee directly employed by that QSA Company) to perform any QSA Services, is considered to be subcontracting and requires prior written consent by PCI SSC in each instance. This applies whether or not the subcontracted entity or individual is already a QSA Company or an Assessor-Employee of a different QSA Company.

The QSA Company must also provide to PCI SSC proof of bound insurance coverage for all such subcontractors to demonstrate policies are in accordance with QSA Program insurance coverage requirements (see Appendix B of the *QSA 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 subcontractor, contact the QSA Program Manager at qsa@pcisecuritystandards.org.*

3.5.3 Insurance

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

Prior to qualification as a QSA Company and annually thereafter, the QSA Company must provide a certificate to PCI SSC from each insurance company as evidence that all required insurance is in force for each region and country with respect to which it is qualified by PCI SSC. 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 USD)
- Commercial General Liability Insurance ($1,000,000 USD minimum, $2,000,000 USD annual aggregate) including:
  - Products
  - Completed Operations
  - Advertising Injury
  - Personal Injury
  - Contractual Liability Insurance
- Commercial Automobile Insurance ($1,000,000 USD minimum limit)
- Crime/Fidelity Bond, both first and third party ($1,000,000 USD minimum for each loss and annual aggregate)
- Technology Errors and Omissions, Cyber-Risk, and Privacy Liability Insurance ($2,000,000 USD minimum for each loss and annual aggregate)

3.6 Primary Contact

The QSA 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 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 an Assessor-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 QSA Agreement.

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

3.7 Assessor Portal

Upon qualification as a QSA Company, access to the Assessor Portal (Portal) is granted to the Primary Contact by e-mail request to the QSA Program Manager. Assessor-Employees receive log-on instructions upon passing the QSA training exam, and PCI SSC enters their grades into the database. Note that Primary Contacts receive a higher-level access than QSA Employees.

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

The Portal includes the following information:

- Editable version of the Reporting Templates (ROC, AOC)
- Library of published Assessor Newsletters
- Recorded webinars
- QSA certificates
- Annual CPE entry and requalification training page
- Primary Contact name, e-mail, and address
- Individual certifications—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 Assessor-Employees
- Insurance policies with respective expiration dates
- Business Regions and the expiration date for each
- Complete list of all QSAs and respective expiration dates
- Addresses for all QSA training locations throughout the year

Each Assessor-Employee and Primary Contact is responsible for checking the Portal on a regular basis for new information and updates.

3.8 FAQs and Guidance Documents

Assessor-Employees should refer to the Frequently Asked Questions (FAQ) section of the Website to obtain further guidance on questions relating to PCI DSS Assessments. The Website should be monitored regularly as information is updated frequently. RSS feed updates are available for the Document Library on 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.*

Assessor-Employees should be familiar 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.

4 PCI DSS Assessment Process

> ***Note:*** *Merchants and service providers should consult with their acquirer or Participating Payment Brands to confirm what PCI DSS validation and reporting method is applicable to them.*

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

PCI DSS Assessments are required to be conducted by a QSA Company through its QSA Employees (and assisting Associate QSA Employees, if applicable) in accordance with the PCI DSS, which contains requirements, testing procedures, and guidance to ensure that the intent of each requirement is understood. QSA Employees must work only on those PCI SSC Assessments for which the QSA Employee is properly qualified by PCI SSC, having appropriate skills, including technology and language, and having an appropriate understanding of the Customer's/Client's business.

The QSA Employee (with assistance of Associate QSA Employees if applicable) document in the ROC the results of the PCI DSS Assessment, including which portions of the PCI DSS Assessment were conducted onsite. The ROC must accurately represent the assessed environment and the security controls that were tested and validated by the QSA Employee (and if applicable, assisting Associate QSA Employees).

4.1 Documenting a PCI DSS Assessment

For each PCI DSS Assessment, the resulting *Report on Compliance* (ROC) must follow the most current *ROC Reporting Template* available on the Portal. The ROC must be accompanied by an Attestation of Compliance (AOC), available in the Document Library on the Website. A duly authorized officer of the QSA Company must sign the AOC, which summarizes whether the entity that was assessed is or is not in compliance with the PCI DSS, and any related findings.

The intent of requiring a signature from a "duly authorized officer" is to ensure that the QSA 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 QSA Company to sign such documents on the QSA Company's behalf and should be competent and knowledgeable regarding the Program and related requirements and duties. Each organization is different and is ultimately responsible for defining its own policies and job functions based on its own needs and culture.

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

The AOC is submitted to the requesting entity/entities according to applicable Participating Payment Brand rules.

The QSA Company must inform the applicable Customer when an Associate QSA Employee has been assigned to work in connection with the PCI DSS Assessment of that Customer, and what parts of the PCI DSS Assessment the Associate QSA Employee will be participating in.

4.2 PCI DSS Assessment Evidence Retention

As per Section 4.5 “Evidence (Assessment Workpaper) Retention” of the *QSA Qualification Requirements*, QSA Companies must gather evidence to support the contents of each ROC. The QSA Company must secure and maintain, for a minimum of three (3) years, 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 DSS Assessment. This information must be available upon request by PCI SSC and its affiliates. The QSA Company must also provide a copy of the evidence-retention policy and procedures to PCI SSC upon request. In cases where an Associate QSA Employee participates in the PCI DSS Assessment, the Lead QSA should ensure that a copy of the completed AQSA Engagement Summary is maintained as part of the workpapers.

If a Customer refuses to provide the QSA Company with the documentary evidence—for example, because it contains information that is sensitive or confidential to the Customer—the QSA Company and the Customer should work together to ensure that the evidence is retained securely at the Customer site and as required by the *QSA Qualification Requirements*, including being made available upon request by PCI SSC for a minimum of three (3) years after completion of the applicable PCI DSS Assessment. It is recommended that the QSA 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 QSA Agreement.

Even if the actual, documented evidence is to be retained by the Customer, the QSA Company must still keep records to identify the specific evidence that was used during the PCI DSS Assessment—for example, digital and/or hard copies of the documents or testing results that are being retained by the Customer. The QSA 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 QSA Company should retain enough Information to ensure that the complete, actual evidence used during the PCI DSS 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”) QSA Program audit process (“QSA Audit”) and in other AQM quality assurance (“QA”) review work as needed, it is common for AQM to request both the QSA Company’s Workpaper Retention Policy and a sample of PCI DSS Assessment workpapers. This is to ensure the QSA Company has a current documented, implemented Workpaper Retention process consistent with the requirements defined in the *QSA Qualification Requirements*—including appropriate level of detailed instructions for Assessor-Employees to comply with. AQM may additionally request blank and/or executed copies of the QSA Company’s Workpaper Retention Policy agreement that each Assessor-Employee is required to sign, and may request additional evidence to demonstrate that all Assessment Results and Related Materials (defined in the QSA Agreement) relating to the PCI DSS 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 ROC for that PCI DSS Assessment.

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

5 Assessor Quality Management Program

The QSA Company must have implemented an internal quality assurance program as documented in its *Quality Assurance Manual*. If participating in the AQSA Program, the QSA Company must additionally maintain and adhere to its *AQSA Mentor Manual*. PCI SSC's Assessor Quality Management (AQM team, or AQM) performs a variety of activities to monitor assessor quality, including review of the *QSA Annual QA Questionnaire*, QSA Audits, and AQSA Spot-Check Audits.

5.1 QSA Annual QA Questionnaire

QSA Companies must annually complete the QSA Annual QA Questionnaire for quality monitoring purposes. The QSA Company will be notified of PCI SSC's request for the QSA Company to complete the QSA Annual QA Questionnaire, via the Portal. Failure to respond in the timelines specified within the QSA Annual QA Questionnaire documentation provided at that time may be considered a Violation (as defined in the *QSA Qualification Requirements*) and may result in remediation or revocation of the QSA Company.

The notification sent to the Primary Contact specifies the information and materials the QSA Company must provide as part of the *QSA Annual QA Questionnaire*, which may include but is not limited to internal QA manuals, documented processes, such as the Workpaper Retention Policy, ROC excerpts redacted in accordance with PCI SSC policy, and other data specified in the notice. The notification will further provide a link to a worksheet that the Primary Contact can use to gather data for submission in the Portal.

The AQM team will review the completed *QSA Annual QA Questionnaire* to monitor the QSA Company's on-going adherence to program requirements and provide relevant feedback in a summary document within the Portal.

***Note:** Findings discovered within the QSA Annual QA Questionnaire review may impact a QSA Company's prioritization for QSA Audit and/or AQSA Spot-Check Audit.*

5.2 QSA Audit and AQSA Spot-Check Audit

As part of QSA Audits, the AQM team performs a holistic review of the QSA Company's internal documentation required by the *QSA Qualification Requirements*, as well as reviews of ROCs to provide reasonable assurance that the documentation of testing procedures performed is sufficient to demonstrate compliance. Refer to *Appendix A* to understand sample criteria against which QSA Companies are measured during QSA Audits.

A QSA Audit by the 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 QSA Company/Employee's on-going adherence to the current *QSA Qualification Requirements*; (2) that the QSA Company's quality policy documentation is implemented and maintained according to the *QSA Qualification Requirements*; and (3) the QSA Company/Employee's on-going general adherence to reporting requirements as evidenced by sampled 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 QSA Company/Employee's on-going adherence to the current *QSA Qualification Requirements*; (2) that the QSA Company's quality policy documentation is implemented and maintained according to the *QSA Qualification Requirements*; and (3) the QSA Company/Employee's on-going general adherence to reporting requirements as evidenced by sampled 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 QSA Audit, including possible Violations. This finding will result in Remediation and/or Revocation, per the current *QSA Qualification Requirements*. Audit findings that result in an Unsatisfactory finding mean that AQM could not confirm one or more of the following: (1) the QSA Company/Employee's on-going adherence to the current *QSA Qualification Requirements*; (2) that the QSA Company's quality policy documentation is implemented and maintained according to the *QSA Qualification Requirements*; and (3) the QSA Company/Employee's on-going general adherence to reporting requirements as evidenced by sampled ROCs.

In addition to reviewing the QSA Company's *Mentor Manual* upon initial entry into the Associate QSA Program, AQM will perform spot audits for QSA Companies participating in the Associate QSA Program. Refer to *Appendix B* for information regarding criteria against which QSA Companies participating in the Associate QSA Program are measured.

For further details on the Assessor Quality Management Program, see the *QSA Qualification Requirements*.

5.3 Ethics

The QSA 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 SSC 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.

QSA Companies and Assessor-Employees are prohibited from performing PCI DSS 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.

QSA Companies and Assessor-Employees must not enter into any contract with a Customer that guarantees a compliant ROC.

Note: *Assessor-Employees are permitted to be employed by only one QSA Company at any given time.*

QSA Companies must fully disclose in the *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 QSA Company, or to which the QSA Company owns the rights, or that the QSA Company has configured or manages.

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

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

5.4 Feedback Process

At the start of each PCI DSS Assessment, the QSA Company must direct the Customer to the *QSA 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 DSS Assessment.

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

Link to the *QSA Feedback Form*:
https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors_feedback

5.5 Remediation Process

QSA Companies that do not meet all applicable quality assurance standards set by PCI SSC (including but not limited to those related to participation in the Associate QSA Program, if applicable), may be offered the option to participate in PCI SSC's QSA Company Quality Remediation program ("Remediation"). PCI SSC may offer Remediation in connection with any quality assurance audit, any Violation, 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 calendar days.
- QSA Company listing on the QSA List updated to "red" to notify merchants/service providers.
- An AQM case manager assigned to the QSA Company to offer support as it works to bring its quality level to the required baseline standard of quality.
- The expectation of strong commitment from the QSA Company to achieve successful completion.
- Fees for review of work.

5.6 Revocation Process

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

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

***Note:** Revocation of QSA Company or Assessor-Employee qualification results in automatic Revocation of all other PCI SSC qualifications that require QSA Company or Assessor-Employee qualification (e.g., PA-QSA, QSA(P2PE), PFI).*

Upon notification of pending QSA Company Revocation by PCI SSC, the QSA Company or Assessor-Employee will have 30 calendar days in which to appeal in writing to PCI SSC.

Revocation will result in the QSA Company or Assessor-Employee being removed from the QSA List or search tool, as applicable.

In the event of QSA Company Revocation, the QSA Company must immediately cease all advertising of its QSA Company qualification. It must also immediately cease soliciting for and performing all pending and active assessments unless otherwise instructed by PCI SSC and comply with the post-revocation requirement specified in the QSA Agreement. Refer to the *QSA Qualification Requirements* for details on the Revocation process.

6 General Guidance

6.1 Resourcing / Transfers

The QSA Company is expected to arrange sufficient backup of Assessor-Employee resources so as not to impact a Customer's validation deadlines in the event an assigned Assessor-Employee is unable to complete a PCI DSS Assessment.

An Assessor-Employee may transfer to another company. The following should be noted when an Assessor-Employee moves to a new company:

1. If the new company is not an active QSA Company, the Assessor-Employee's qualification will be inactive until employed by an active QSA Company. Inactive status does not suspend or modify requalification deadlines.
2. If the Assessor-Employee moves to an active QSA Company and is to be utilized by that QSA Company as an Assessor-Employee, the Primary Contact of the new QSA Company must notify the QSA Program Manager prior to permitting the Assessor-Employee to participate in any PCI DSS Assessment. The following information must be provided to the QSA Program Manager:
   - Name
   - E-mail
   - Phone
   - Notification if the Assessor-Employee is acting as a sub-contractor.

6.2 PCI SSC Logos and Marks

Unless expressly authorized, a QSA Company or Assessor-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 QSA Program-specific logo is available on request via e-mail to the QSA 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 DSS compliance. Please note that the PCI logo is a registered trademark and may not be used without authorization. You may not use the phrases or marks: PCI Compliant, PCI Certified, PCI DSS Compliant, PCI DSS Certified, or PCI with a check mark, or any other mark or logo that suggests or implies compliance or conformance with any of the PCI SSC Standards.*

6.3 QSA Company Changes

In the event that a QSA 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—contact the QSA Program Manager for the *Assessor Name Change Request Form*.

6.4 ISA and PCIP Programs

QSA Employees are permitted to transition into the PCI Internal Security Assessor (ISA) Program without taking the ISA training. However, they must be employed by a company that has been approved as a Sponsor Company in accordance with ISA Program requirements.

QSA Employees and AQSA Employees may opt-into the PCI Professional (PCIP) Program. Refer to the instructions and form under the PCIP Program on the Website for details regarding how to apply.

6.5 Participating Organizations

Companies affiliated with the payment card industry globally are able to become PCI Security Standards Council "Participating Organizations."

QSA Companies, Approved Scanning Vendors, and all other entities approved by PCI SSC to assess or otherwise evaluate conformance to any PCI SSC Standard are ineligible to become a Participating Organization, subject to certain exceptions applicable to Related Entity Groups that satisfy applicable requirements regarding separation, independence, and non-integration of business operations. Refer to the *Participating Organization Rights, Obligations and Rules of Participation*, and the *Participating Organization Application*, on the Website.

6.6 Special Interest Groups

The objectives of Special Interest Groups (SIGs) are to provide guidance and tools on best practices for merchants, third parties, and the PCI SSC Assessor community.

Assessor-Employees are welcome to participate in SIGs along with Participating Payment Brands, other PCI SSC Members, Participating Organizations and ASV companies subject to any applicable SIG restrictions and eligibility requirements.

SIG participants are expected to provide expertise and to actively participate and contribute to the end deliverable. Assessor-Employees should allot time to attend meetings and additional time to draft and/or review documents, in accordance with their desired level of participation.

For details on upcoming or in progress SIG meetings and how to sign up refer to *Special Interest Groups* on the Website.

Appendix A Quality Criteria for QSA Audits

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

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

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

	QSA Company Documentation (per the QSA Qualification Requirements)
1	QSA 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	QSA Company's QA Manual includes a requirement for all Assessor-Employees to regularly monitor the Website for updates, guidance and new publications relating to the QSA Program.
3	QSA Company's Code of Conduct Policy supports—and does not contradict—the PCI SSC Code of Professional Responsibility.
4	QSA Company's Conflict of Interest Policy is consistent with PCI SSC guidance and is appropriately available within the QSA Company.
5	QSA Company's Security and Incident Response Policy is consistent with PCI SSC guidance and is appropriately available within the QSA Company.

	Workpapers/Evidence Retention
1	QSA Company's Evidence Retention Policy includes all required content defined within the *QSA 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 QSA Company for all tests that are required to be performed.
3	QSA Company was able to provide a blank copy of the QSA Company's Workpaper Retention Policy, as well as produce copies signed by the Assessor-Employee(s).

	Ethics
1	QSA Company and Assessor-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	QSA Company and Assessor-Employees maintained independence throughout the engagement, and provided adequate reporting as to how this was validated and maintained.

Reporting	
1	QSA Company and Assessor-Employees used the appropriate templates for reports.
2	QSA Company and Assessor-Employees provided clear, consistent detail as to how requirements were validated to be in place, avoiding excessive use of cut and paste.
3	QSA Company and Assessor-Employees provided a compensating control worksheet for each compensating control noted within the ROC reporting.
4	For the high-level diagram, QSA Company and Assessor-Employees addressed all Reporting Instructions, including identification of connected entities.
5	QSA Company and Assessor-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 QSA Company and Assessor-Employees evaluated that the scope was accurate and appropriate, QSA Company and Assessor-Employees included sufficient detail to demonstrate the findings that validated the scope (rather than just the method used)
7	QSA Company and Assessor-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 Quality Criteria for Associate QSA Employee Spot Audits

In addition to reviewing the QSA Company's *Mentor Manual* upon initial entry into the Associate QSA Program (refer to the PCI SSC Website for the most recent version of PCI SSC's *AQSA Mentor Manual Template*), AQM will perform spot audits of QSA Companies participating in the Associate QSA Program. QSA Companies participating in the Associate QSA Program are measured against the following criteria:

- *QSA Company Mentor Manual* (per the *QSA Qualification Requirements*)
- AQSA Development Documentation/Evidence Retention
- Ethics

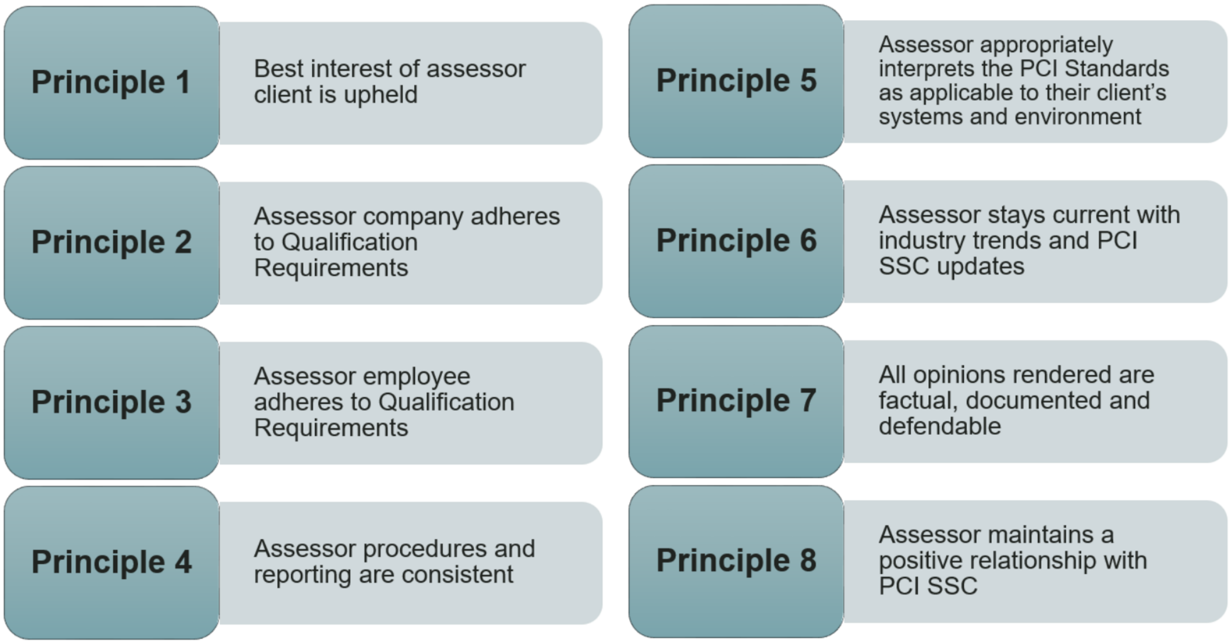
Examples of documents/evidence AQM may seek to validate the above criteria are as follows:

QSA Company Mentor Manual (per the QSA Qualification Requirements)	
1	QSA Company's *Mentor Manual* includes an up-to-date AQSA-Mentor Assignment Log documenting assignments of eligible Mentor QSAs to Associate QSA Employees, with documentation of the reviews within the last 30 days.
2	QSA Company's *Mentor Manual* has a signed Mentor Responsibilities Acknowledgment Form for every Mentor assigned to an Associate QSA Employee.
3	Content in the QSA Company's *Mentor Manual* is specific to the QSA Company and is substantive and implemented.
AQSA Development Documentation/Evidence Retention	
1	Associate QSA Employee is able to provide the completed AQSA Engagement Summary for a sample of PCI DSS Assessments in which the Associate QSA Employee participated.
2	AQSA Skills Summary Form has been updated within the last 90 days to reflect the Associate QSA Employee's quarterly progress.
3	Review of AQSA Engagement Summary forms completed by the Lead QSA indicates all assigned tasks are consistent with the tasks the Associate QSA Program allows Associate QSA Employees to complete.
Ethics	
1	Documentation is available to validate that the Lead QSA—and not just the Associate QSA Employee—went on-site.

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

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

The Eight Guiding Principles are as follows:



Principle 1	Best interest of assessor client is upheld
Principle 2	Assessor company adheres to Qualification Requirements
Principle 3	Assessor employee adheres to Qualification Requirements
Principle 4	Assessor procedures and reporting are consistent
Principle 5	Assessor appropriately interprets the PCI Standards as applicable to their client’s systems and environment
Principle 6	Assessor stays current with industry trends and PCI SSC updates
Principle 7	All opinions rendered are factual, documented and defendable
Principle 8	Assessor maintains a positive relationship with PCI SSC

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, and that they’ve acted in the best interest of the customer in an ethical manner that results in factual, documented, and defendable opinions. Program participants must keep up with PCI SSC updates (included but not limited to updates to the *QSA Qualification Requirements* and *QSA Program Guide*, monthly Assessor Newsletter articles, published FAQs on the Website, and content from the Quarterly Assessor 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.

Appendix D Quality Assurance Best Practices

PCI SSC's approach to quality borrows from the philosophy of Philip B. Crosby in *Quality is Free*: "quality is conformance to requirements," similar to other quality standards, such as ISO 9001. PCI SSC defines its QSA Program requirements primarily in the *QSA Qualification Requirements*, as well as the *QSA Program Guide* and other Program documentation.

This appendix represents some best practices related to Assessor quality assurance and adherence to PCI SSC requirements. Section 4.3.1 of the *QSA Qualification Requirements* provides high-level requirements as to what a QSA Company's internal quality assurance should include, but intentionally leaves many of the details of the implementation to the QSA Company to define. The following sections support QSA Companies as they plan their own quality processes and evaluate implementations.

Documented Quality Assurance Process and Manual

Without limiting any other QSA Requirements, to meet QSA Program expectations, assessor-employees must understand what is expected of them and have the resources to execute all required tasks. The details specified in Section 4.3.1 of the *QSA Qualification Requirements* ensure that QSA Companies have a documented quality assurance process and manual that is maintained and distributed to all Assessor-Employees.

Here are some considerations for evaluating the adequacy of such documentation:

- A "successful" quality process is defined, repeatable, and measurable. The details in the *QA Manual*, for example, must ensure that all QSA Employees and all personnel performing quality assurance review (QA Review) of QSA Services (QA Reviewers) perform their work in a manner consistent with both the documented process and each other. Mature processes reflect precisely that.
- The PCI SSCs requirements are a base minimum, and it is often useful and/or necessary to go beyond the stated requirements to achieve a mature process. Merely restating the verbiage from the *QSA Qualification Requirements* is often inadequate to educate Assessor-Employees on how to actually meet the requirements from within the organization. For example, stating that there is a requirement "for independent quality review of QSA Company and Assessor-Employee work product" without a detailed process as to how to achieve that would not adequately prepare Assessor-Employees to execute to that end.
- PCI SSC recognizes that QSA Companies are not monolithic, and the details specified in Section 4.3.1 of the *QSA Qualification Requirements* are written in a way to allow for very different implementations. For example, QSA Companies may differ greatly in how they implement the above requirement for independent QA Review. While the *QSA Qualification Requirements* require all QA Reviewers to be qualified by PCI SSC as a QSA, AQSA, or PCIP, they do not dictate whether QA Reviewers must be a dedicated team that only reviews work product or instead peer review between QSA Employees; indeed, both approaches can be valid if each QA Reviewer has independence from the PCI DSS Assessment process, and the QA Review process is implemented in a way that otherwise meets the criteria of the *QSA Qualification Requirements*. Additionally, some QSA Companies report success with QA Reviewers who have performed (unrelated) PCI DSS Assessment work in the past, citing the understanding of the process and experience writing the reports as factors that make for a more efficient review timeframe. Others suggest leveraging production QSA Employees to also perform QA as an auxiliary duty in which they rotate periodically, helping ensure QA Reviewers

are keeping up-to-date on the PCI DSS and the QSA Company's practice, while also serving to improve QSA Company reporting.

- Make sure QA Reviewers understand the full scope of the review work, and ensure they are prepared with the knowledge and resources to execute. Section 4.3.1 of the *QSA Qualification Requirements* states that the independent review referred to above "*must cover assessment procedures performed, supporting documentation, information documented in the ROC related to the appropriate selection of system components, sampling procedures, compensating controls, remediation recommendations, proper use of payment definitions, consistent findings, thorough documentation of results, sampled workpaper retention review, and review of servicing markets/qualified regions.*" Some QSA Companies may elect to have "staged reviews" wherein a technical reviewer with relevant experience reviews some or all of the above, while a more general review for writing correctness and clarity is performed by a general QA Reviewer. Other QSA Companies may have one QA Reviewer who is capable of doing both. No matter who does the review, the time allotted must be commensurate with the depth of review expected.
- Keep in mind that quality is not something that only happens at the end of the PCI DSS Assessment when the ROC is being finalized—quality processes should be designed to ensure quality from start-to-finish. The language from the *QSA Qualification Requirements* above makes general reference to scope validation, and by the time the ROC is with a QA Reviewer, it is difficult to change course. Consider a process wherein there is a checkpoint early in the engagement where a skilled, knowledgeable technical reviewer can identify possible gaps in technical work (configuration reviews, etc.) or considerations related to priority topics like scope, sampling rationale, etc. in order for the assessor to address those gaps early rather than as an afterthought or worse, not at all. Once the ROC is complete, the QA Reviewer can then review to ensure the validated scope is consistently documented throughout the ROC.
- Quality must be a priority throughout the PCI DSS Assessment. It is important to implement supports to ensure that processes are being documented to monitor the QSA Employee's assessment work and reporting for quality issues. This could include periodic checks on a QSA Employee's assessment process through a manager or a more senior QSA Employee to ensure quality and consistency, as well as periodic a "ride-along" by a manager or a more senior QSA Employee. Furthermore, the documented quality process could define criteria by which QSA Employees are prioritized for such monitoring, such as new hires, QSA Employees who have received negative feedback, or QSA Employees who receive excessive and/or consistent feedback from QA Reviewers.
- Processes should treat QA Review as a meaningful exercise and should consider how to proceed with and document situations, such as disagreement between a QA Reviewer and the QSA Employee who performed the assessment, as well as excessive and/or repeat findings. How are disagreements mediated? How is unresolved feedback documented, and how is the ROC finalized without relevant change? Is there a process for a manager to work with the QSA Employee to improve persistent issues without simply relying on the QA Reviewer to catch the error every time? Is feedback from QA Reviewers considered part of the QSA Employee's overall performance?

Checklists for QA Review

While not mandatory, some QSA Companies report good results using a checklist to keep track of what the QA Reviewer must review during each PCI DSS Assessment QA Review, with the executed checklist retained with assessment workpapers. Such a checklist can aid in establishing a mature process wherein QSA Employees and QA Reviewers perform consistent work and ensure that tasks are completed by all parties involved.

Though not exhaustive, the following are examples of items that QSA Employees have found useful to include in a QA Review checklist:

- Are the correct documents in use? For example, latest *ROC Reporting Template*, AOC, etc.
- Are all documents complete? Reporting, tick marks, and signatures are filled in, as appropriate?
- Review for format, spelling, and/or grammar (as applicable)? Use of the *ROC Reporting Template* is mandatory and may be personalized consistent with the most recent version of the *FAQs for use with the ROC Reporting Template* document. While PCI SSC does not review ROCs and AOCs for spelling or grammar, these are professional documents, and excessive or egregious typos and misspellings may raise questions about accuracy and precision of reporting. QSA Companies may have their own style guides for a standard approach for things like date format. PCI SSC does not define date format requirements at this time, and therefore, would emphasize consistency; that is, use the same date format throughout the report.
- Overall, the goal of the QA Review process is to ensure that reporting is logical, accurate, and not contradictory to anything else in the ROC or AOC. The process should provide reasonable assurance that the PCI DSS Assessment was performed completely and correctly, and that anyone reading the report will understand the security of the environment. Does reporting adequately communicate what testing was performed and the results observed to allow someone to reproduce them?
- Has scope been validated either by the QA Review or a separate technical reviewer, and does it match what is documented throughout the ROC?
- Does the sampling rationale make sense in the context of factors, such as sample size vs. total population? If the QSA Company has a defined a sampling method, is the sampling present in the PCI DSS Assessment consistent with that method? If the QSA Employee is performing a subsequent year’s assessment, have samples other than those from previous years’ assessments been reviewed?
- Are there any identified gaps in technical work, such as configuration reviews, for the various technologies included in the cardholder data environment (CDE)?
- Are diagrams readable? Are they current? Are there any inconsistencies or contradictions with other stated reporting?
- Do overall descriptions of systems and processes make sense? Are there any inconsistencies or contradictions with other stated reporting?
- Throughout the report, is there consistency for documentation reviewed, personnel interviewed, sample sets, and so on.? Do the descriptions in the requirements match the items listed in the tables within the Summary Overview section?
- If the QSA Company is performing a subsequent year’s assessment for an entity, even if a different QSA Employee is used, is the reporting different from the year before? Copying and pasting content from previous years’ assessments can raise suspicions about the quality of assessment. Copied information may no longer be valid, thus raising concerns that a new assessment has not been fully performed.

- Has there been review of collected workpaper evidence? Has workpaper evidence been retained consistent with the QSA Company's Workpaper Retention Policy? Do evidence file names match the document names listed in the tables in the Summary Overview? Does workpaper evidence meet the control requirements' validation expectations?

Again, this is not an exhaustive list of examples; any checklist should also reflect updates from communications from PCI SSC, such as the Assessor Newsletter and published FAQs, as well as feedback received from payment card brands, acquirers, and others.

Evaluation and Evolution of Quality Processes

Evaluation of quality processes can take several forms, and the need for change and/or evolution of existing processes may be driven by various factors. For example, the need for change may be identified in the course of implementation. Process changes may be required in communications from PCI SSC, such as the Assessor Newsletter or published FAQs. Change may be required under the QSA Company's documented process for periodic internal review to address the requirement in Section 4.3.1 of the *QSA Qualification Requirements*: "*The QSA Company must have qualified personnel conduction internal periodic checks, at least annually, of the QA Program to monitor effectiveness.*"

Asking questions as part of QA Review, or more generally, may reveal the need for process improvements and evolution. Consider the following questions:

- Does the QA Review process result in reporting that is logical, accurate, and not contradictory to anything else in the ROC or AOC? Does the process provide reasonable assurance that the assessment was performed completely and correctly, and that anyone reading the report will understand the security of the environment? Does reporting adequately communicate what testing was performed and the results observed to allow someone to reproduce them?
- Are QSA Employees learning from the process and avoiding repeat findings or errors, or do some assessors consistently have the same findings or the same errors? Are the QA Reviewers' observations resulting in training for assessors, both so they can learn from their mistakes and from those of their peers as well? This is easily one of the most significant ways for QSA Companies to be more consistent in their reporting.
- What activities do QA Reviewers do to calibrate their reporting expectations to ensure that a reviews by Reviewer X and Reviewer Y will generally result in the same findings? For example, do they periodically review the same reports to compile feedback and learn from each other's findings?
- Is workpaper evidence retention occurring consistently with the QSA Company's Workpaper Retention Policy? If the client has chosen to hold their evidence, has such evidence been made accessible on-demand?

As part of the requirement in *QSA Quality Requirements*, Section 4.3.1, regarding periodic internal checks of the QSA Company's QA Program to monitor effectiveness, it is expected that evidence is available upon request to PCI SSC to ensure on-going compliance with the requirement.