Payment Card Industry (PCI)
Qualified Security Assessors

Program Guide
Version 2.0

December 2017

Document Changes

Date	Version	Description
November 2016	1.0	This is the 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.

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 4 below, or in the QSA 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 publically 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

3 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.

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. All such documents are available on the Website:

Term	Definition / Source / Document Reference
AOC	Refer to the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* (Glossary).
Assessor-Employee	Refer to QSA Qualification Requirements
Associate QSA Employee (AQSA)	Refer to QSA Qualification Requirements.
Associate QSA Program (or 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	Refer to the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* (Glossary).
CPE	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	Refer to Glossary.
Primary Contact	Refer to QSA Agreement.
QSA Agreement	Appendix A to 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.

Term	Definition / Source / Document Reference
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.
Payment Application	Refer to Glossary.
Participating Payment Brand	Refer to QSA Agreement.
PCI DSS Assessment	Refer to QSA Qualification Requirements.
PCI SSC	PCI Security Standards Council, which manages the PCI SSC Standards.
Remediation	The correction of vulnerabilities identified within an information system.
ROC	Refer to Glossary.
SAQ	Refer to 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.

5 Roles and Responsibilities

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

5.1 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.

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 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 8 titled "Assessor Quality Management" for additional information.

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

5.3 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.
- 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 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 QSA Companies and Assessor-Employees are strongly encouraged to check the FAQs published on the Website prior to contacting PCI SSC with questions.*

5.4 Customers / Clients

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.

6 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. Refer to Section 6.2 for more information on the Associate QSA Program.

Only those QSA Companies and QSA Employees qualified by PCI SSC and included in 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 the performance of PCI DSS Assessments as further described in this document.

6.1 Requalification

All QSA Companies must be requalified regionally by PCI SSC on an annual basis. The annual QSA Company 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, 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*. Assessor-Employee requalification requires proof of applicable Continuing Professional Education (CPE), proof of training successfully completed, and payment of annual training fees.

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 one-year requalification for a certification with a current qualification date of 15 November 2017 will be changed to 15 November 2018 upon successful completion regardless of whether the requalification was completed on 31 October 2017 or 25 November 2017.

6.1.1 Requalification Timeframe

In an effort 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 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 QSA Employee (or AQSA, as applicable) candidate.

6.2 Associate QSA Program

The goal of the Associate QSA Program is to provide a path to enable QSA Companies to develop new resources into fully qualified QSA Employees, through formal mentorship and monitored skills development. Associate QSA Employees are qualified by PCI SSC to support QSA Employees on PCI DSS Assessments. Refer to Section 3.3 of the QSA Qualification Requirements for more details on entry-level requirements for AQSAs.

Note: *PCI SSC does not qualify Associate QSA Employees to support any standard other than the PCI DSS.*

An Associate QSA Employee is able to apply to become a fully qualified QSA Employee once they meet the 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 what parts of the PCI DSS Assessment the Associate QSA Employee will be participating in. 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 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.

6.2.1 Associate QSA Duties

Each QSA Company 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 QSAC'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 with 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 AOCs
- Validating the scope of a PCI DSS assessment
- Selection of systems and systems components where sampling is used
- Evaluating compensating controls
- Initiating and leading compliance discussions with payment brands or acquirers

6.2.2 Mentor Program and Mentor Manual Template

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 PCI SSC 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 365 days; 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 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 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 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 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 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.

6.3 Assessor-Employee Continuing Professional Education (CPE)

In order to remain "in Good Standing," all Assessor-Employees must provide proof of information systems audit training within the last 12 months of the requalification date in accordance with the current version of the *PCI SSC CPE Maintenance Guide*.

An Assessor-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 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 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 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.

6.4.1 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 act as a QSA Company in any capacity—outside of the qualified region(s).

  For example, if a Merchant is headquartered in the US and has satellite offices in-scope for PCI DSS located in Singapore, the QSA Company must be qualified in both USA and Asia Pacific before they are permitted to perform QSA Services for the merchant.
- If QSA-related tasks must be performed outside of the qualified region it may be necessary to engage a QSA Company qualified for that region to perform the related tasks. Refer to 6.4.2, “Subcontracting,” below.
- To add or remove a region, contact the QSA Program Manager at PCI SSC. Added regions will appear on the QSA List on the Website pending receipt of payment fees and evidence of insurance.

6.4.2 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 aspect of the services to be performed in connection with any PCI DSS Assessment, 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 given subcontractor, please contact the QSA Program Manager at qsa@pcisecuritystandards.org.*

6.4.3 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 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 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)
- 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)

6.5 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. 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 an Assessor-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 QSA Agreement.

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

6.6 Assessor Portal

Access to the Portal is granted once the QSA Company is qualified as a QSA Company. Assessor-Employees receive log-on instructions upon passing the QSA 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 QSA Program Manager.

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

The Portal includes the following information:

- Editable version of the ROC Reporting Template
- Library of published Assessor Newsletters
- Recorded Webinars
- QSA Certificates in PDF format
- Annual CPE entry and requalification training page
- 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 Assessor-Employees
- Insurance policies with respective expiration dates
- Business Regions and the expiration date for each
- Complete list of all QSAs and their expiration dates
- Addresses for all QSA training locations throughout the year

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

6.7 FAQs and Guidance Documents

Assessor-Employees should refer to the Frequently Asked Questions (FAQ) section of the PCI SSC Website to obtain further guidance on questions relating to PCI DSS 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.*

Assessor-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 DSS Assessment Process

To demonstrate compliance with the PCI DSS, merchants and service providers 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.

The QSA Employee (with assistance of Associate QSA Employees if applicable) will 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 evaluated by the QSA Employee (and if applicable, assisting Associate QSA Employees).

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. If onsite assessment and ROC is the appropriate method, they should also confirm the acceptable method of reporting per their acquirer or the Participating Payment Brands.*

7.1 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 Website. The ROC must be accompanied by an Attestation of Compliance (AOC), available in the Documents 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 QSA Employee also signs the AOC. 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.

7.2 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.

8 Assessor Quality Management Program

The QSA Company must have implemented an internal quality assurance program as documented in its Quality Assurance Manual. As part of QSA Audits, Assessor Quality Management (AQM) at PCI SSC 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 PCI 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 to the QSA Agreement. 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, please see the QSA Qualification Requirements document available on the Website.

8.1 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.

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

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

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.*

8.2 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 payment card 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 Feedback Form:
https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors_feedback

8.3 Remediation Process

QSA 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 QSA Company Quality Remediation program ("Remediation"). PCI SSC may offer Remediation in connection with any quality assurance audit, any violation (as defined in the QSA 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.
- 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 expected baseline standard of quality.
- The expectation of strong commitment from the QSA Company to achieve successful completion.
- Fees for review of work.

8.4 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.
- Violation of any provision regarding non-disclosure of confidential materials.
- Failure to maintain at least one certified QSA 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 QSA Company Revocation by PCI SSC, the QSA Company or Assessor-Employee will have 30 days in which to appeal the ruling in writing to PCI SSC.

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 and P2PE QSA).*

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

9 General Guidance

9.1 Resourcing /Transfers

The QSA Company is expected to arrange sufficient back-up 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 should be supplied to the QSA Program Manager:
   - Name
   - E-mail
   - Phone
   - Notification if the Assessor-Employee is acting as a sub-contractor.

9.2 PCI SSC Logo

Unless expressly authorized, a QSA Company or Assessor-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 QSA Program-specific logo is available on request via e-mail to the QSA Program Manager.

9.3 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—please contact the QSA Program Manager for the *Assessor Name Change Request Form.*

9.4 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.

9.5 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 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, 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.