## Document Changes

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 2016</td>
<td>1.0</td>
<td>This is the first release of the QSA Program Guide.</td>
</tr>
</tbody>
</table>
# Table of Contents

DOCUMENT CHANGES .................................................................................................................. 2  
1 INTRODUCTION ......................................................................................................................... 5  
2 RELATED PUBLICATIONS ......................................................................................................... 5  
3 UPDATES TO DOCUMENTS AND SECURITY REQUIREMENTS ............................................. 6  
4 TERMINOLOGY ......................................................................................................................... 7  
5 ROLES AND RESPONSIBILITIES ............................................................................................... 8  
  5.1 PARTICIPATING PAYMENT BRANDS .................................................................................... 8  
  5.2 PCI SECURITY STANDARDS COUNCIL ............................................................................. 8  
  5.3 QUALIFIED SECURITY ASSESSOR COMPANIES (QSA COMPANIES) ....................... 9  
  5.4 CUSTOMERS / CLIENTS ....................................................................................................... 10  
6 QSA QUALIFICATION PROCESS ............................................................................................ 11  
  6.1 QSAmployee Requalification ............................................................................................ 11  
    6.1.1 Requalification Timeframe ......................................................................................... 11  
  6.2 CONTINUING PROFESSIONAL EDUCATION (CPE) ........................................................ 12  
  6.3 FEES .................................................................................................................................... 12  
    6.3.1 Regions ....................................................................................................................... 12  
    6.3.2 Subcontracting ............................................................................................................ 13  
    6.3.3 Insurance .................................................................................................................... 13  
  6.4 PRIMARY CONTACT ............................................................................................................. 14  
  6.5 ASSESSOR PORTAL .............................................................................................................. 14  
  6.6 FAQs AND GUIDANCE DOCUMENTS ................................................................................. 15  
7 PCI DSS ASSESSMENT PROCESS ............................................................................................ 16  
  7.1 DOCUMENTING A PCI DSS ASSESSMENT ................................................................. 16  
  7.2 PCI DSS ASSESSMENT EVIDENCE RETENTION ............................................................. 17  
8 ASSESSOR QUALITY MANAGEMENT PROGRAM ..................................................................... 18  
  8.1 ETHICS ............................................................................................................................... 18  
  8.2 FEEDBACK PROCESS ......................................................................................................... 19  
  8.3 REMEDIATION PROCESS .................................................................................................. 19  
  8.4 REVOCATION PROCESS .................................................................................................... 20
## 9 GENERAL GUIDANCE

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>RESOURCING / TRANSFERS</td>
<td>21</td>
</tr>
<tr>
<td>9.2</td>
<td>PCI SSC LOGO</td>
<td>21</td>
</tr>
<tr>
<td>9.3</td>
<td>QSA COMPANY CHANGES</td>
<td>21</td>
</tr>
<tr>
<td>9.4</td>
<td>PARTICIPATING ORGANIZATIONS</td>
<td>21</td>
</tr>
<tr>
<td>9.5</td>
<td>SPECIAL INTEREST GROUPS</td>
<td>22</td>
</tr>
</tbody>
</table>
1 Introduction

This Program Guide provides information to the Primary Contact at QSA Companies and other QSA Employees pertinent to their roles in connection with the PCI SSC Qualified Security Assessor (QSA) program (the “Program”). The Program is more fully described in QSA Qualification Requirements on the Website, and capitalized terms used but not otherwise defined herein are defined in the QSA Qualification Requirements. Companies wishing to apply for QSA Company status should first consult the QSA Qualification Requirements.

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.

<table>
<thead>
<tr>
<th>Document name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPE Maintenance Guide</td>
<td>Provides the number of CPEs required on an annual basis by assessors to remain certified.</td>
</tr>
<tr>
<td>Lifecycle for Changes to PCI DSS and PA-DSS</td>
<td>Describes the development cycle for the PCI DSS and PA-DSS.</td>
</tr>
<tr>
<td>Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures (“PCI DSS”)</td>
<td>Lists the specific technical and operational security requirements and provides the assessment procedures used by assessors to validate PCI DSS compliance.</td>
</tr>
<tr>
<td>PCI DSS Glossary of Terms, Abbreviations, and Acronyms (the “Glossary”)</td>
<td>Lists and defines the specific terminology used in the PCI DSS.</td>
</tr>
<tr>
<td>PCI SSC Programs Fee Schedule</td>
<td>Lists the current fees for specific qualifications, tests, retests, training, and other services.</td>
</tr>
<tr>
<td>PCI DSS Qualification Requirements for Qualified Security Assessors (QSAs) (“QSA Qualification Requirements”)</td>
<td>Defines the baseline set of requirements that must be met by a QSA Company and QSA Employees in order to perform PCI DSS Assessments.</td>
</tr>
<tr>
<td>PCI DSS Template for Report on Compliance (“ROC Reporting Template”)</td>
<td>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.</td>
</tr>
<tr>
<td>PCI SSC Information Supplements</td>
<td>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.</td>
</tr>
<tr>
<td>Document name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>QSA Feedback Form</td>
<td>Gives the customer an opportunity to offer feedback regarding the QSA and the assessment process.</td>
</tr>
<tr>
<td></td>
<td><a href="https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors_feedback">https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors_feedback</a></td>
</tr>
</tbody>
</table>

### 3 Updates to Documents and Security Requirements

PCI SSC updates the PCI DSS and other PCI SSC Standards according to a standards life cycle management process. 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 QSA 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, 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:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition / Source / Document Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOC</td>
<td>Refer to the <em>PCI DSS Glossary of Terms, Abbreviations, and Acronyms</em> (Glossary).</td>
</tr>
<tr>
<td>CDE</td>
<td>Refer to the <em>PCI DSS Glossary of Terms, Abbreviations, and Acronyms</em> (Glossary).</td>
</tr>
<tr>
<td>CPE</td>
<td>Continuing Professional Education.</td>
</tr>
<tr>
<td>Good Standing</td>
<td>Refer to QSA Qualification Requirements.</td>
</tr>
<tr>
<td>PA-DSS</td>
<td>Refer to Glossary.</td>
</tr>
<tr>
<td>Primary Contact</td>
<td>Refer to QSA Agreement.</td>
</tr>
<tr>
<td>QSA Agreement</td>
<td>Appendix A to QSA Qualification Requirements.</td>
</tr>
<tr>
<td>QSA Company</td>
<td>Refer to QSA Qualification Requirements.</td>
</tr>
<tr>
<td>QSA Employee</td>
<td>Refer to QSA Qualification Requirements.</td>
</tr>
<tr>
<td>QSA Requirements</td>
<td>Refer to QSA Qualification Requirements.</td>
</tr>
<tr>
<td>QSA List</td>
<td>The then-current list of QSA Companies published by PCI SSC on the Website.</td>
</tr>
<tr>
<td>QSA PM</td>
<td>QSA Program Manager contact e-mail <em><a href="mailto:qsa@pcisecuritystandards.org">qsa@pcisecuritystandards.org</a></em>.</td>
</tr>
<tr>
<td>Payment Application</td>
<td>Refer to Glossary.</td>
</tr>
<tr>
<td>Participating Payment Brand</td>
<td>Refer to QSA Agreement.</td>
</tr>
<tr>
<td>PCI DSS Assessment</td>
<td>Refer to QSA Qualification Requirements.</td>
</tr>
<tr>
<td>PCI SSC</td>
<td>PCI Security Standards Council, which manages the PCI SSC Standards.</td>
</tr>
<tr>
<td>Remediation</td>
<td>The correction of vulnerabilities identified within an information system.</td>
</tr>
<tr>
<td>ROC</td>
<td>Refer to Glossary.</td>
</tr>
<tr>
<td>SAQ</td>
<td>Refer to Glossary.</td>
</tr>
<tr>
<td>Security Issue</td>
<td>Refer to QSA Qualification Requirements.</td>
</tr>
<tr>
<td>Website</td>
<td>The then-current PCI SSC Website (and its accompanying web pages), which is currently available at <a href="http://www.pcisecuritystandards.org">www.pcisecuritystandards.org</a>.</td>
</tr>
</tbody>
</table>
5 Roles and Responsibilities

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

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:

- Defining merchant and service provider levels
- Managing compliance enforcement programs (requirements, mandates or dates for compliance)
- Establishing penalties and fees
- Establishing validation process requirements (onsite PCI DSS Assessment with ROC or self-assessment with SAQ) 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 QSA 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: Contact details for the Participating Payment Brands can be found in FAQ #1142 on the Website.

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 QSA 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 QSA Qualification Process

In an effort to help ensure that each QSA Company and QSA 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.

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.

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.

6.1 QSA Employee Requalification

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

Each QSA Employee must be requalified by PCI SSC on an annual basis. The annual requalification date is based upon the QSA Employee’s previous qualification date. Requalification requires proof of Continuing Professional Education (CPE), proof of training successfully completed, and payment of annual training fees.

For example, a one-year requalification for a certification with a current qualification date of 15 March 2016 will be changed to 15 March 2017 upon successful completion regardless of whether the requalification was completed on 29 February 2016 or 25 March 2016.

6.1.1 Requalification Timeframe

In an effort to help ensure adequate time to complete requalification requirements, QSA Employees should note:

- Registration for requalification training must be completed (and approved, where applicable) prior to the QSA Employee’s expiration date. A candidate who is not registered prior to their expiry date must re-enrol 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 certified during this time and will not be recertified until the requalification exam is completed and passed.

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

Note: Negative feedback from Customers (merchants, service providers, etc.), PCI SSC, Participating Payment Brands, or others may impact the QSA Company and/or QSA Employee’s eligibility for requalification.
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 to the QSA Program as a new candidate.

6.2 Continuing Professional Education (CPE)

In order to remain “in good standing,” QSA 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.

A QSA Employee must earn a minimum of 20 CPE credits per year and a minimum of 120 CPE credits per rolling three-year period.

6.3 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.

6.3.1 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 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 within that region to perform the related tasks. Refer to 6.4.3, “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.
6.3.2 Subcontracting

A QSA Company's engagement, hiring, or other use of any other company, organization, or individual (other than a QSA 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 a QSA 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.

6.3.3 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)
6.4 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 a QSA Employee.

Notices from PCI SSC to the designated Primary Contact may be communicated via the secure web 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 SSC in a timely manner.

6.5 Assessor Portal

Access to the Assessor Portal is granted once the QSA Company is activated. QSA Employees receive log-on instructions upon passing the QSA 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 Assessor Portal: https://programs.pcissc.org/

The Assessor 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 QSA 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.
6.6 FAQs and Guidance Documents

QSA 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 on the Website.

QSA 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 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 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.

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.

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.
7.2 PCI DSS Assessment Evidence Retention

As per Section 4.5 “Evidence (Assessment Workpaper) Retention” of the QSA Qualification Requirements, QSA Companies are expected to 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.

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 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 QSA Audit and in other QA review work as needed, it is common for Assessor Quality Management (AQM) team at PCI SSC to request both the QSA Company’s Workpaper Retention Policy and a sample of 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 QSA Employees to comply with. AQM may additionally request blank and/or executed copies of the QSA Company’s Workpaper Retention Policy agreement that each QSA 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 a quality assurance program as documented in its Quality Assurance Manual. Assessor Quality Management (AQM) at PCI SSC reviews ROCs to ensure that the documentation of testing procedures performed is sufficient to demonstrate compliance.

An 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. Call the 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 warning letter will be sent with specific opportunities for improvement and other improvement activities. 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 letter is sent with specific opportunities for improvement. Mandatory call with the 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.

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 QSA 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 QSA 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 QSA 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 QSA 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 90 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 QSA 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.
- P2PE QSA or any other PCI SSC required training.
- Cheating on any exam in connection with QSA, PA-QSA, P2PE QSA or any other PCI SSC required training.

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

Revocation will result in the QSA Company or QSA Employee being removed from the QSA List.

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.

Re-application cannot be made for 180 days. In order to reapply, there must be evidence of improvement in the internal QA program and any other identified requirements.

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

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

9.1 Resourcing/Transfers

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

A QSA Employee may transfer to another company. The following should be noted when a QSA Employee moves to a new company:

1. If the company they are transferring to is not an active QSA Company, their qualification will be inactive until they are employed by an active QSA Company.

2. If the QSA Employee moves to an active QSA Company, the Primary Contact of the new QSA Company should notify the QSA Program Manager immediately. The following information should be supplied to the QSA Program Manager:
   - Name
   - E-mail
   - Phone
   - Notification if the QSA Employee is acting as a sub-contractor.

9.2 PCI SSC Logo

Unless expressly authorized, a QSA Company or QSA 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 Participating Organization members in the PCI Security Standards Council.

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.

QSA Employees are welcome to participate in SIGs along with Participating Payment Brands, other PCI SSC Members, Participating Organizations, and ASV companies.

SIG participants are expected to provide expertise and to actively participate and contribute to the end deliverable. QSA 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 see Special Interest Groups on the Website.