Payment Card Industry (PCI)

Qualification Requirements

For Payment Application Qualified Security Assessors (PA-QSA)

Version 2.0
February 2014

Document Changes

Date	Version	Description
February 2014	2.0	Made minor changes to this document to be consistent with v3.0 of the PCI Data Security Standards. Qualifications required for entry are more precise and include a requirement for application development experience. The PA-QSA Company Testing Laboratory section now provides more explanation and Appendix B has been replaced for use in qualifying for the Program and for annual re-qualification. Section on AQM has been updated. PA-QSA Feedback Form and Fee Schedule are now on-line.

Table of Contents

1 Introduction

In addition to creating the PCI DSS, members of the payment card industry (“PCI”) have adopted the *Payment Application Data Security Standard* (the "PA-DSS," as further defined herein), a set of requirements derived from and closely related to the PCI DSS, but intended to illustrate for payment software vendors what is required for their Payment Applications (defined below) to facilitate and not prevent their customers’ PCI DSS compliance. The PA-DSS is maintained by PCI SSC (defined below) and is available through the Website (defined below).

These *PA-QSA Qualification Requirements* supplement the *QSA Qualification Requirements* (defined below) for each QSA Company that intends to qualify as a Payment Application Qualified Security Assessor Company (defined below), and describes the minimum capability requirements, laboratory requirements, and related documentation that a QSA Company must satisfy and provide to PCI SSC in order to qualify to perform PA-DSS Assessments (defined below). These *PA-QSA Qualification Requirements* amend, restate, and supersede in its entirety the *Payment Card Industry (PCI) Data Security Standard QSA Validation Requirements Supplement for Payment Application Qualified Security Assessors (PA-QSAs), v1.2 (April 2008).*

1.1 Terminology

Throughout these *PA-QSA Qualification Requirements*, the following terms shall have the following meanings:

Term	Meaning
PA-DSS	The then-current version of the *Payment Card Industry (PCI) Payment Application Data Security Standard Requirements and Security Assessment Procedures,* as from time to time amended and made available on the Website.
PA-DSS Assessment	With respect to a given PA-QSA Company, such PA-QSA Company’s review of a Payment Application for purposes of validating the compliance of such Payment Application with the PA-DSS as part of the PA-DSS Program.
PA-DSS Program	The Payment Application Data Security Standard Program managed and operated by PCI SSC.
PA-QSA	Acronym for "Payment Application – Qualified Security Assessor" Company, a company then qualified by PCI SSC to perform PA-DSS Assessments.
PA-QSA Addendum	The *Addendum to Qualified Security Assessor (QSA) Agreement for Payment Application QSAs* attached as Appendix A to the *PA-QSA Qualification Requirements*.
PA-QSA Company	A company that has been qualified, and continues to be qualified, by PCI SSC to perform PA-DSS Assessments for PA-DSS Program purposes.
PA-QSA Company Testing Laboratory	A laboratory environment maintained by the PA-QSA Company to perform testing of payment applications that software vendors provide for validation.

Term	Meaning
PA-QSA Employee (or PA-QSA employee)	An individual who is employed by a PA-QSA Company and has satisfied and continues to satisfy all PA-QSA Requirements applicable to employees of PA-QSA Companies who will conduct PA-DSS Assessments, as described in further detail herein.
PA-QSA List	The then-current list of PA-QSA Companies published by PCI SSC on the Website.
PA-QSA Qualification Requirements	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Qualification Requirements for Payment Application Qualified Security Assessors (PA-QSA)*, as from time to time amended and made available on the Website.
PA-QSA Requirements	With respect to a given PA-QSA Company or PA-QSA Employee, the requirements and obligations thereof pursuant to the *PA-QSA Qualification Requirements*, the *PA-QSA Addendum*, the *PA-DSS Program Guide*, each addendum, supplement, and other agreement entered into between such PA-QSA Company or PA-QSA Employee and PCI SSC, and any and all other policies, procedures, requirements, or obligations imposed, mandated, provided for, or otherwise established by PCI SSC from time to time in connection with any PCI SSC program in which such PA-QSA Company or PA-QSA Employee (as applicable) is then a participant, including but not limited to, the requirements of all applicable PCI SSC training programs, quality assurance and remediation programs, program guides, and other related PCI SSC program materials.
Payment Application	A software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties.
PCI DSS Assessment	An Assessment (as defined in the *QSA Agreement*).
PCI SSC	PCI Security Standards Council, LLC.
QSA Agreement	The *PCI Qualified Security Assessor (QSA) Agreement* attached as Appendix A to the *QSA Qualification Requirements*.
QSA Qualification Requirements	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Qualification Requirements for Qualified Security Assessors (PA-QSA)*, as from time to time amended and made available on the Website.
Vendor	A software vendor that develops and sells, distributes, or licenses its Payment Application to a third party.
Website	The then-current PCI SSC Web site (and its accompanying Web pages), which is currently available at http://www.pcisecuritystandards.org.

All capitalized terms used in these *PA-QSA Qualification Requirements* without definition shall have the meanings specified in the *QSA Qualification Requirements* or the *QSA Agreement*, as applicable.

1.2 Goal

To be qualified and remain in "good standing" (defined in the *PA-QSA Addendum*) as a PA-QSA Company by PCI SSC, a QSA Company and its QSA Employees must, among other things, meet or exceed all applicable PA-QSA Requirements as well as the general requirements for all QSA Companies and its QSA Employees as set forth in the *QSA Qualification Requirements* and the *QSA Agreement* (all such general QSA requirements, collectively, "QSA Requirements"), and the PA-QSA Company must have in effect a current *PA-QSA Addendum* with PCI SSC. Companies that qualify as PA-QSA Companies are identified on the PA-QSA List in accordance with the *PA-QSA Addendum*.

Together, the QSA Requirements and the PA-QSA Requirements are intended to serve as a **qualification baseline** and provide a transparent process for PA-QSA Company and PA-QSA Employee qualification and re-qualification for PA-DSS Program purposes. Among other things, the PA-QSA Company and PA-QSA Employees must adhere to all requirements in these *PA-QSA Qualification Requirements* and must provide all of the required provisions described herein.

1.3 Qualification Process Overview

The PA-DSS Program qualification process first involves the qualification of the QSA Company, followed by qualification of the QSA Company's employee(s) who will be performing and/or managing the PA-DSS Assessments.

All PA-QSA Companies appear on the PA-QSA List. If a company is not on this list, its work product as a PA-QSA Company is not recognized by PCI SSC. PA-QSA Companies and PA-QSA Employees must re-qualify annually.

To initiate the qualification process, the QSA Company must sign the *PA-QSA Addendum* in unmodified form and submit it to PCI SSC.

1.4 Document Structure

This document (among other things) defines the requirements a QSA Company must meet to become a PA-QSA Company. The document is structured in five sections as follows.

Section 1: Introduction offers a high-level overview of the PA-DSS Program application process.

Section 2: PA-QSA Company Business Requirements covers minimum business requirements that must be demonstrated to PCI SSC by the QSA Company that are additional to those required by QSA Companies. This section outlines information and items that must be provided to establish required business stability, independence, and insurance coverage.

Note:

All requirements set forth in the QSA Qualification Requirements *must be met by organizations wishing to qualify as PA-QSA Companies.*

Section 3: PA-QSA Company Capability Requirements reviews the information and documentation necessary to demonstrate the QSA Company's service expertise, as well as that of its employees.

Section 4: PA-QSA Company Administrative Requirements focuses on the standards to meet regarding the logistics of doing business as a PA-QSA Company, including background checks, adherence to PCI SSC procedures documented in the *PA-DSS Program Guide,* quality assurance, and protection of confidential and sensitive information.

1.5 Related Publications

This document should be used in conjunction with the current, publically available version of the following other PCI SSC publications (or successor documents), each available through the PCI SSC Website:

- *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures*
- *Payment Card Industry (PCI) Data Security Standard Qualification Requirements for Qualified Security Assessors (QSA)*
- *Payment Card Industry (PCI) Payment Application Data Security Standard Requirements and Security Assessment Procedures*
- *Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS) Program Guide*

1.6 PA-QSA Application Process

In addition to outlining the requirements that a PA-QSA Company and its PA-QSA Employees must meet to be recognized by PCI SSC to perform PA-DSS Assessments, this document describes the information that must be provided to PCI SSC as part of the PA-DSS Program application and qualification process. Each outlined requirement is followed by the information that must be submitted to document that the QSA Company meets or exceeds the stated requirements.

To facilitate preparation of the application package, refer to Appendix C: PA-DSS Program – Application Process Checklist. All application materials and the signed *PA-QSA Addendum* must be submitted in English. The *PA-QSA Addendum* is binding in English even if the *PA-QSA Addendum* was translated and reviewed in another language. All other documentation provided by the PA-QSA Company in a language other than English must be accompanied by a certified English translation (examples include business licenses and insurance certificates).

All PA-DSS Program application packages must include a signed *PA-QSA Addendum* and the required documentation. Applicants should send their completed application packages by mail to the following address:

PCI SSC
401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone number: 1-781-876-8855

E-mail submissions will not be accepted.

Important Note: PCI SSC reserves the right to reject any application from any applicant (company or employee) that PCI SSC determines has committed, within two (2) years prior to the application date, any conduct that would have been considered a “Violation” for purposes of the *QSA Qualification Requirements* or *QSA Agreement* if committed by a QSA Company or QSA Employee. The period of ineligibility will be a minimum of one (1) year, as determined by PCI SSC in a reasonable and non-discriminatory manner, in light of the circumstances.

1.7 Additional Information Requests

In an effort to maintain the integrity of the PA-DSS Program, PCI SSC may from time to time request that PA-QSA Companies and PA-QSA Employees submit additional information or materials in order to demonstrate adherence to applicable requirements or as part of the applicable qualification or re-qualification process. PA-QSA Companies are required to respond to each such request with the required information or documentation no later than three (3) weeks from receipt of the corresponding written request.

2 Payment Application QSA Company Business Requirements

This section describes the minimum business requirements and related information that must be provided to PCI SSC. The provisions requested include information about the company's business legitimacy, independence, and required insurance coverage.

2.1 Business Legitimacy

PA-QSAs must meet all business legitimacy requirements as set forth in the *QSA Qualification Requirements.*

2.2 Independence

PA-QSAs must meet all independence requirements as set forth in the *QSA Qualification Requirements.*

2.3 Insurance Coverage

PA-QSAs must meet all insurance coverage requirements as set forth in the *QSA Qualification Requirements.*

2.4 PA-DSS Program Fees

2.4.1 Requirement

Each PA-QSA Company must provide to PCI SSC all fees required by PCI SSC in connection with the PA-QSA Company's (or its PA-QSA Employees') participation in the PA-DSS Program (collectively, "PA-DSS Program Fees"), including without limitation, remediation and related fees, and the following:

- An initial application fee (see the Website – PCI SSC Programs Fee Schedule). Initial application fees are credited toward regional qualification fees (see below) if a company is qualified as a PA-QSA Company. Initial application fee checks should be made payable to PCI SSC and mailed with the completed PA-QSA application package. See Section 1.6 of this document for the mailing address.
- Regional qualification fees, which must be paid in full within 60 days of notification, and depend on the region or country in which the PA-QSA Company intends to perform PA-DSS Assessments.
- Annual PA-QSA Company regional re-qualification fees for subsequent years, which depend on the region or country in which the PA-QSA Company intends to perform PA-DSS Assessments.
- For each PA-QSA Employee, fees for required PCI SSC annual training.

Note:

The current initial application, regional qualification, and training fees are specified on the Website—see PCI SSC Programs Fee Schedule—and are subject to change.

2.5 PA-QSA Agreements

2.5.1 Requirement

As described in further detail in the *QSA Qualification Requirements*, each QSA Company must have executed and submitted the *QSA Agreement* to qualify as a QSA Company.

Once qualified as a QSA Company, there are various other agreements a QSA Company must execute and submit to PCI SSC, depending on the QSA programs in which the QSA wishes to participate. In order to become qualified under any such other PCI SSC program, a QSA Company must fulfill the applicable requirements for that program, including the requirements and provisions of that program's Qualification Requirements document

In order to participate in the PA-DSS Program, PCI SSC requires that all agreements between PCI SSC and the PA-QSA Company (including the *PA-QSA Addendum*) be signed by a duly authorized officer of the PA-QSA Company, submitted in unmodified form to PCI SSC, and submitted with the completed PA-QSA Company application package.

The *PA-QSA Addendum* requires, among other things, that the PA-QSA Company and its PA-QSA Employees comply with all applicable PA-QSA Requirements.

3 PA-DSS Program Capability Requirements

3.1 PA-QSA Company – Services and Experience

3.1.1 Requirements

- The PA-QSA Company must fulfill all QSA Requirements, as defined in the *QSA Agreement*.
- The PA-QSA Company must fulfill all PA-QSA Requirements and comply with all terms and provisions of the PA-QSA's *QSA Agreement*, *PA-QSA Addendum* and any other agreements executed with PCI SSC.
- The PA-QSA Company must have performed at least two PCI DSS Assessments.
- The PA-QSA Company must possess substantial application security knowledge and experience performing application and/or code reviews, as determined in the sole discretion of PCI SSC.
- The PA-QSA Company must have demonstrated competence in cryptographic techniques, to include cryptographic algorithms, key management and rotation processes, and secure key storage, as determined in the sole discretion of PCI SSC.
- The PA-QSA Company must have demonstrated competence in using penetration-testing methodologies, to include use of forensic tools/methods, ability to exploit OWASP vulnerabilities, and ability to execute arbitrary code to test processes.

3.1.2 Provisions

The following information must be provided to PCI SSC:

- For the PA-QSA Company, a description of both relevant experience with application security and application and code reviews, preferably related to payment applications and including a description of methodology used to perform such reviews equal to at least one year or three separate application security engagements.
- A description of dates and clients for two previous PCI DSS Assessments performed by the PA-QSA Company.
- Description of the PA-QSA Company's relevant areas of specialization within application security, and code reviews (for example, use of OWASP or other secure coding guidelines, web vulnerability assessment, application penetration testing, or designing or implementing cryptography systems), demonstrating at least one area of specialization.
- Description of the PA-QSA Company's experience with cryptographic techniques, including cryptographic algorithms, key management and rotation processes, and secure key storage, demonstrating at least one area of specialization.
- Description of the PA-QSA Company's experience using penetration testing methodologies, to include use of forensic tools/methods, ability to exploit OWASP vulnerabilities, and ability to execute arbitrary code to test processes.
- Two client references from application security engagements within the last 12 months.

3.2 PA-QSA Employee – Skills and Experience

Each PA-QSA Employee performing or managing PA-DSS Assessments must be qualified by PCI SSC as *both* a QSA Employee and a PA-QSA Employee; only PA-QSA Employees qualified by PCI SSC can conduct PA-DSS Assessments. PA-QSA Employees are responsible for the following:

- Performing the PA-DSS Assessments.
- Verifying that the laboratory used to test the client's application meets requirements defined in Appendix B: Confirmation of PA-QSA Company's General Testing Laboratory Capabilities.
- Verifying the work product addresses all assessment procedure steps and supports the validation status of the application.
- Strictly following the PA-DSS and *PA-DSS Program Guide.*
- Producing the final report.

3.2.1 Requirements

Each PA-QSA Employee performing or managing PA-DSS Assessments must also:

- Be a QSA Employee and fulfill all requirements specified in Section 3.2 of the *QSA Qualification Requirements*.
- Have performed at least two PCI DSS Assessments.
- Have substantial application security knowledge and experience that demonstrates at least three (3) years of work experience, with a minimum of one year of experience in each of the following disciplines:
    - Conducting application testing and source-code reviews, performing web vulnerability assessments, performing application penetration testing, experience using penetration-testing methodologies including the use of forensic tools/methods.
    - Source-code creation per OWASP or other secure coding guidelines, ability to exploit OWASP vulnerabilities, and ability to execute arbitrary code to test processes; and
    - Demonstrated competence in cryptographic techniques such as cryptographic algorithms, key management and rotation processes, and secure key storage, as determined in the sole discretion of PCI SSC.
- Be knowledgeable about the PA-DSS, as determined in the sole discretion of PCI SSC.
- Attend annual training provided by PCI SSC, and legitimately pass, of his or her own accord without any unauthorized assistance, all examinations conducted as part of training. If a PA-QSA Employee fails to pass any exam in connection with such training, the PA-QSA Employee must no longer lead or manage a PA-DSS Assessment until successfully passing the exam on a future attempt.
- Be employees of the PA-QSA Company (meaning this work cannot be subcontracted to non-employees) unless PCI SSC has given prior written consent for each subcontracted worker.

Approved subcontractors shall not be permitted to include a company logo other than that of the responsible PA-QSA Company or any reference to another company in the *Report of Validation* or attestation documents while performing work on behalf of the PA-QSA Company.

3.2.2 Provisions

Note: *This section is intended to draw out specific experience from each individual seeking to be qualified as a PA-QSA Employee. The individual must provide examples (including the timeframe) of how their work experience meets the PA-DSS Program requirements. This section is intended to measure the individual's skills against the required skills.*

The following information must be provided to PCI SSC for each individual seeking to be qualified as a PA-QSA Employee, in addition to the QSA Employee information required in Section 3.2:

- A description that includes dates and clients, of two previous PCI DSS Assessments performed by such individual.
- A description of experience or work examples of such individual within secure application development, source-code reviews and application testing, and cryptography with at least three (3) years of work experience, with a minimum of one year of experience in each of the following disciplines:
  - Conducting application testing and source-code reviews, performing web vulnerability assessments, performing application penetration testing, experience using penetration testing methodologies including the use of forensic tools/methods
  - Source code creation per OWASP or other secure coding guidelines, ability to exploit OWASP vulnerabilities, and ability to execute arbitrary code to test processes
  - Demonstrated competence in cryptographic techniques such as cryptographic algorithms, key management and rotation processes, and secure key storage, as determined in the sole discretion of PCI SSC.

3.3 PA-QSA Company's Testing Laboratory

Use of a Testing Laboratory is mandatory for the testing of Payment Applications that customers submit for validation for PA-DSS Program purposes. PA-QSA Companies are required to implement, use and maintain their own internal PA-QSA Company Testing Laboratory for PA-DSS Assessment purposes. If the PA-QSA Company's own PA-QSA Company Testing Laboratory is not used to test a Payment Application for PA-DSS Program purposes, then an alternate testing laboratory, such as the applicable Vendor's testing laboratory, can be used. The alternate laboratory must meet the same Objectivity Criteria (described below) as the PA-QSA Company's Testing Laboratory.

Requirements for using a Testing Laboratory during a PA-DSS Assessment can be found in the *PA-DSS Program Guide*. Submission of Appendix B: Testing Laboratory Configuration for PA-DSS Assessments as set forth in the *ROV Reporting Template* is required for each PA-DSS Assessment.

The Objectivity Criteria for the PA-QSA Company's Testing Laboratory are as follows:

- **PCI DSS compliant**

  In order to simulate real-world merchant environments, the PA-QSA Company's Testing Laboratory must be configured to be PCI DSS compliant. All security technologies required by the PCI DSS, as well as operating systems, supporting software, and any patches, must be configured in a PCI DSS compliant manner.

  The PA-QSA Company must assign responsibility for PA-QSA Company Testing Laboratory maintenance to ensure that processes and controls are in place to ensure that system components, applications, source code, documentation, and other laboratory assets can be accessed only by authorized personnel.

- **Vulnerability Scanning and Penetration Testing**

  The PA-QSA Company Testing Laboratory must include capabilities for vulnerability scanning and penetration testing of applications including:

  - Use of forensic tools/methods capable of searching all storage and output identified for evidence of sensitive authentication data
  - Attempting to exploit application vulnerabilities per PA-DSS Requirement 5
  - Running of arbitrary code during application update processes

- **Testing Laboratory Verification**

  PCI SSC reserves the right to conduct audits of the PA-QSA Company's Testing Laboratory at any time and further reserves the right to conduct site visits at the expense of the PA-QSA Company and at the discretion of PCI SSC.

3.3.1 Requirement

The PA-QSA Company must complete Appendix B of this document as part of the PA-DSS Program application process, to confirm that the PA-QSA Company:

a) Maintains a PA-QSA Company Testing Laboratory meeting all requirements specified in Appendix B of this document; and

b) Has documented processes to verify that an alternative laboratory (such as a third-party lab service or a Vendor's laboratory) meets the requirements specified in Appendix B, whenever it is necessary to use an alternative testing laboratory.

In addition, a PA-QSA Employee must review and confirm Testing Laboratory configurations as part of each PA-DSS Assessment and complete Appendix B: Testing Laboratory Configuration for PA-DSS Assessments in the *PA-DSS ROV Reporting Template*.

3.3.2 Provisions

- Description of documented processes used to verify that the alternate laboratory meets the requirements specified in Appendix B, whenever it is necessary to use an alternate testing laboratory rather than the PA-QSA Company's Testing Laboratory.
- Completed *PA-QSA Qualification Requirements* Appendix B: Confirmation of PA-QSA Company's General Testing Laboratory Capabilities.

3.4 Mock Assessment

3.4.1 Requirement

PCI SSC reserves the right to require successful completion of a mock assessment annually, after at least one employee has successfully completed PA-QSA training (including passing the training examination), or to use a mock assessment as a tool to validate the PA-QSA Company's quality assurance program.

4 PA-QSA Company Administrative Requirements

This section describes the administrative requirements for PA-QSA Companies, including company contacts, background checks, adherence to PCI SSC procedures, quality assurance, and protection of confidential and sensitive information.

4.1 Contact Person

4.1.1 Requirement

The PA-QSA Company must provide PCI SSC with a primary and secondary contact:

- Person responsible for PA-DSS Assessments.
- Person responsible for oversight of quality assurance of PA-DSS Assessments.

4.1.2 Provisions

The following contact information must be provided to PCI SSC, for both primary and secondary contacts:

- Name
- Job Title
- Address
- Phone number
- Fax number
- E-mail address

4.2 Background Checks

Each PA-QSA Employee must meet all background check requirements as specified in the *QSA Qualification Requirements.*

4.3 Adherence to PCI Procedures

4.3.1 Requirements

- The Report on Validation must follow the procedures documented in the *PA-DSS Program Guide.*
- An officer of the PA-QSA Company must sign the *PA-QSA Addendum*, which includes a statement that the PA-QSA Company will adhere to all PA-QSA Requirements.
- Prior to conducting any PA-DSS Assessment for a given payment application Vendor, the PA-QSA Company must inform such Vendor that the Vendor must execute and deliver to PCI SSC a standard Vendor Release Agreement on the form approved by PCI SSC in order for any of its payment applications to be identified on PCI SSC's published List of Validated Payment Applications.

4.4 Quality Assurance

4.4.1 Requirements

- The PA-QSA Company must fulfill all QSA Company requirements for quality assurance as defined in Section 4.4 of the *QSA Qualification Requirements*.
- The PA-QSA Company must have an implemented PA-QSA quality assurance program, documented in a quality assurance manual.
- The PA-QSA Company must provide a PA-QSA Feedback Form to each PA-DSS Assessment client during the course of the PA-DSS Assessment. The PA-QSA Feedback Form is an on-line form available on the PCI SSC Website.
- The PA-QSA Company must comply with all PA-DSS Program quality assurance requirements established from time to time.
- PCI SSC reserves the right to conduct audits of the PA-QSA Company at any time and further reserves the right to conduct site visits at the expense of the PA-QSA Company and at the discretion of PCI SSC.
- Upon request, the PA-QSA Company must provide the quality assurance manual to PCI SSC.

4.4.2 Provisions

The PA-QSA Company must provide the following to PCI SSC:

- The description of the responsibilities of the PA-DSS Company quality assurance person that lists, at a minimum, the following responsibilities:
  - Oversight of quality assurance for all PA-DSS Assessment work documentation.
  - Review and approval of all ROVs prior to submission to PCI SSC.
  - Sole responsibility for submitting ROVs to the web portal designated for such purpose by PCI SSC.
  - A description of the contents of the PA-QSA Company's quality assurance manual to confirm the procedures fully document the PA-QSA Company's PA-DSS Assessment and report review processes for generation of ROVs as required pursuant to the requirements contained in the *PA-DSS Program Guide*, including a requirement that all PA-QSA Employees must adhere to the PA-DSS.

4.5 Protection of Confidential and Sensitive Information

PA-QSA Companies must adhere to all requirements to protect sensitive and confidential information, as required by PCI SSC, including but not limited to the provisions of Section 4.5 of the *QSA Qualification Requirements.*

4.6 Evidence Retention

PA-QSA Companies must meet all evidence retention requirements as set forth in the *QSA Qualification Requirements*.

Additionally, for a minimum of three (3) years from submission of a given ROV to PCI SSC, the PA-QSA Company must secure (in accordance with 4.5 above) and maintain documented evidence (whether in digital or hard copy format) substantiating all conclusions in such ROV, including but not limited to copies of any and all case logs, audit results, work papers, notes, and technical information created and/or obtained during the applicable PA-DSS Assessment. For examples of acceptable forms of evidence, please see Appendix D: Examples of Evidence.

4.7 PA-QSA Company Recognition of Payment Application Validation Status

4.7.1 Requirements

The PA-QSA Company must not provide any formal recognition of PA-DSS validation status to a client until PCI SSC has notified the PA-QSA Company and Vendor as follows:

- PCI SSC has issued a notification of acceptance to both the PA-QSA Company and the Vendor; and
- PCI SSC has included the Vendor and specific application on the published List of Validated Payment Applications.

4.7.2 Provisions

The PA-QSA Company must provide the following:

- A statement that the PA-QSA Company will not recognize a Payment Application's validation status until PCI SSC has notified the PA-QSA Company and the applicable Vendor via a notification of acceptance and inclusion of the application on the List of Validated Payment Applications.

5 PA-QSA Initial Qualification and Annual Re-qualification

For information about the process after initial qualification, please refer to Section 6.3 of the *PA-DSS Program Guide.*

The annual re-qualification process for the PA-DSS Program requires an annual submission of Appendix B: Confirmation of PA-QSA Company's General Testing Laboratory Capabilities.

Appendix A: Addendum to Qualified Security Assessor (QSA) Agreement for Payment Application QSAs

A.1 Introduction

This Addendum to Qualified Security Assessor (QSA) Agreement for Payment Application QSAs (the "Addendum") is entered into by and between PCI Security Standards Council, LLC ("PCI SSC") and the undersigned Applicant ("QSA") as of the date of PCI SSC's signature below (the "Addendum Effective Date"), for purposes of adding and modifying certain terms of the Qualified Security Assessor (QSA) Agreement between PCI SSC and QSA dated as of the QSA Agreement Date below, as in effect on the Addendum Effective Date (the "Agreement").

In consideration of the mutual covenants herein set forth, the adequacy and sufficiency of which is acknowledged, QSA and PCI SSC agree as follows.

A.2 General Information

Applicant			
Applicant Name:			
Company Name:			
QSA Agreement Date:			
Location/Address:			
City:		State/Province:	
Country		Postal Code:	
Regions Applying For (see Website for list):			
Applicant's Signature			
Applicant's Officer Signature ↑		*Date ↑*	
Applicant Officer Name:		Title:	

For PCI SSC Use Only:			
Application Date:			
Application Approved:			
PCI SSC Officer Signature ↑			
PCI SSC Officer Name:		Title:	

A.3 Terms and Conditions

A.3.1 Definitions

All capitalized terms used but not defined in this Addendum shall have the meanings ascribed to them in the Agreement or the *PA-QSA Qualification Requirements* (defined below), as applicable. Additionally, while this Addendum is in effect, the following terms appearing in the Agreement are hereby amended as follows for purposes of the Agreement:

(a) The term "Services" shall include (without limitation) the PA-QSA Services (defined below).

(b) The term "QSA Requirements" shall include (without limitation) the PA-QSA Requirements.

(c) The terms “Subjects” or “QSA Company clients” shall include (without limitation) Vendors.

(d) The terms "Report of Compliance," "ROC" and "Attestation of Compliance" shall, where applicable, include (without limitation) the terms "Report of Validation," "ROV" and "Attestation of Validation," respectively, as those terms are used in the *PA-QSA Qualification Requirements.*

A.3.2 PA-QSA Services

Subject to the terms and conditions of this Addendum and the Agreement, PCI SSC hereby approves QSA, while QSA is in “good standing” (defined in Section A.5(b) below) as a PA-QSA Company (or as otherwise expressly approved by PCI SSC in writing) to conduct PA-DSS Assessments for Vendors solely in order to validate compliance of such Vendors’ Payment Applications with the PA-DSS. Notwithstanding the foregoing, QSA agrees that neither QSA nor PCI SSC shall recognize any Payment Application's validation status until (a) such Vendor has signed a standard Vendor Release Agreement on the form approved for Vendors by PCI SSC for vendors participating in the PA-DSS Program (a “VRA”), (b) PCI SSC has notified QSA and such Vendor of such validation via an acceptance letter signed by PCI SSC, and (c) such Vendor's Payment Application has been listed on PCI SSC's published List of Validated Payment Applications.

QSA agrees to monitor the Website at least weekly for changes to the PA-DSS, the *PA-QSA Qualification Requirements* and/or the *PA-DSS Program Guide*. QSA will incorporate all such changes into all PA-DSS Assessments initiated on or after the effective date of such changes. QSA acknowledges that PCI SSC will not accept any Report of Validation ("ROV") regarding a PA-DSS Assessment that is not conducted in accordance with the PA-DSS in effect at the initiation date of such PA-DSS Assessment.

For purposes of this Addendum, "PA-QSA Services" means PA-DSS Assessments and all other services provided by QSA to PCI SSC and/or Vendors in connection with this Addendum or the PA-DSS Program; and “PA-QSA Qualification Requirements” means the then-current version of (or successor documents to) the *Payment Card Industry (PCI) Qualification Requirements for Payment Application Qualified Security Assessors (PA-QSA)*, as from time to time amended and made available on the Website.

A.3.3 Performance of PA-QSA Services

(a) QSA warrants, represents, and agrees that it will perform each PA-DSS Assessment in strict compliance with the PA-DSS in effect as of the commencement date of such PA-DSS Assessment and that QSA shall comply with all applicable PA-QSA Requirements and QSA Requirements. Without limiting the foregoing, QSA will include along with each ROV submitted to PCI SSC an Attestation of Validation in the form available through the Website signed by a duly authorized officer of QSA, in which QSA certifies without qualification that (a) in performing the applicable PA-DSS Assessment, QSA followed the PA-DSS without deviation, and (b) application of such procedures did not indicate any conditions of non-compliance with the PA-DSS other than those noted in the ROV.

(b) QSA acknowledges and agrees that, in an effort to maintain the integrity of the PA-DSS Program, PCI SSC from time to time may request demonstrated adherence to the PA-DSS and the *PA-QSA Qualification Requirements*. Each such request shall be in writing, and QSA shall respond thereto with documented evidence of such adherence in form and substance acceptable to PCI SSC no later than three (3) weeks from QSA's receipt of such written request.

(c) QSA agrees that, prior to performing any PA-DSS Assessment with respect to a given Payment Application, QSA shall obtain an executed VRA from the applicable Vendor, and QSA shall deliver such executed VRA to PCI SSC as soon as possible thereafter but, in any event, no later than the date upon which QSA delivers to PCI SSC the corresponding ROV generated in connection with such PA-DSS Assessment.

A.3.4 PA-QSA Service Staffing

QSA shall ensure that a PA-QSA Employee that is fully qualified in accordance with all applicable provisions of the *PA-QSA Qualification Requirements* supervises all aspects of each engagement to perform PA-QSA Services in accordance with the *PA-QSA Qualification Requirements* and the PA-DSS.

A.3.5 PA-QSA Requirements

QSA agrees to adhere to all PA-QSA Requirements, and in connection therewith, to comply with all requirements and make all provisions as set forth in the *PA-QSA Qualification Requirements,* including without limitation, all business, capability and administrative requirements, as set forth in Sections 2, 3 and 4 of the *PA-QSA Qualification Requirements,* and all requirements with respect to PA-QSA Employees (as defined in the *PA-QSA Qualification Requirements*). Further, QSA warrants that, to the best of QSA's ability to determine, all information provided to PCI SSC in connection with this Addendum and QSA's participation in the PA-DSS Program is and shall be accurate and complete as of the date such information is provided. QSA acknowledges that PCI SSC may from time to time require QSA to provide a representative to attend any mandatory training programs in connection with the PA-DSS Program, which may require the payment of attendance and other fees.

A.4 PA-DSS Program Fees

QSA shall pay all applicable fees in connection with participation in the PA-DSS Program as referenced in and in accordance with the *PA-QSA Qualification Requirements.* QSA acknowledges that PCI SSC may review and modify such fees at any time and from time to time, provided that PCI SSC shall notify QSA of such change and such change will be effective thirty (30) days after the date of such notification. Should QSA not agree with any such change, QSA may terminate this Addendum upon written notice to PCI SSC at any time within such 30-day period.

A.5 QSA List; Promotional References; Restrictions

(a) So long as QSA is qualified by PCI SSC as a PA-QSA Company, PCI SSC may, at its sole discretion, identify QSA as such on the QSA List or in such other publicly available list(s) of PA-QSA Companies as PCI SSC may maintain and/or distribute from time to time, whether on the Website or otherwise (for purposes of the Agreement, such other list (if any) shall be deemed to be part of the QSA List), along with information identifying QSA and corresponding qualification status information (including without limitation, good standing, remediation, and/or revocation status).

Without limiting the rights of PCI SSC set forth in the preceding sentence or elsewhere, PCI SSC expressly reserves the right to remove QSA from the QSA List (or any other PCI SSC list) at any time when QSA is not in good standing as a PA-QSA Company.

(b) So long as QSA is in good standing as a PA-QSA Company and is identified in the QSA List as a PA-QSA Company, QSA may make reference to such PA-QSA Company listing and its qualification as a PA-QSA Company in advertising or promoting its PA-QSA Services. A PA-QSA Company is deemed to be in "good standing" as a PA-QSA Company as long as the PA-QSA Addendum between the PA-QSA Company and PCI SSC is in full force and effect, the PA-QSA Company has been approved by PCI SSC as a PA-QSA Company and such approval has not been revoked, terminated, suspended, cancelled, or withdrawn, the PA-QSA Company is in compliance with all PA-QSA Requirements, and the PA-QSA Company is not in breach of any of the terms or conditions of remediation, its PA-QSA Addendum (including without limitation, all provisions regarding compliance with the PA-QSA Qualification Requirements, and payment) or any other agreement with PCI SSC.

(c) QSA shall not: (i) make any false, misleading, or incomplete statements regarding, or misrepresent PCI SSC, its status as a PA-QSA Company or the requirements of the PA-DSS, including without limitation, any requirement regarding the implementation of the PA-DSS or the application thereof to any Vendor, or (ii) state or imply that the PA-DSS requires usage of QSA's products or services.

A.6 Vendor Data; Quality Assurance

(a) To the extent any data or other information obtained by QSA relating to any Vendor in the course of providing PA-QSA Services thereto may be subject to any confidentiality restrictions between QSA and such Vendor, QSA must provide in each agreement containing such restrictions (and in the absence of any such agreement must agree with such Vendor in writing) that (i) QSA may disclose each ROV, Attestation of Validation and other related information to PCI SSC and/or its Members, as requested by the Vendor, (ii) to the extent any Member obtains such information in accordance with the preceding clause A.6(a)(i), such Member may disclose (a) such information on an as needed basis to other Members and to such Members' respective Financial Institutions and Issuers and to relevant governmental, regulatory and law enforcement inspectors, regulators and agencies and (b) that such Member has received a ROV and other related information with respect to such Vendor (identified by name) and whether the ROV was satisfactory, and (iii) QSA may disclose such information as necessary to comply with its obligations and requirements pursuant to Section A.10.2(b) of the Agreement. Accordingly, notwithstanding anything to the contrary in Section A.6.2(a) of the Agreement, to the extent requested by a Vendor, PCI SSC may disclose Confidential Information relating to such Vendor and obtained by PCI SSC in connection with this Addendum to Members in accordance with this Section A.6(a), and such Members may in turn disclose such information to their respective member Financial Institutions and other Members. QSA hereby consents to such disclosure by PCI SSC and its Members. As between any Member, on the one hand, and QSA or any Vendor, on the other hand, the confidentiality of ROVs and any other information provided to Members by QSA or any Vendor is outside the scope of the Agreement and may be subject to such confidentiality arrangements as may be established from time to time between such Member, on the one hand, and QSA or such Vendor (as applicable), on the other hand.

(b) Notwithstanding anything to the contrary in Section A.6 of the Agreement or in this Addendum, in order to assist in ensuring the reliability and accuracy of PA-DSS Assessments, QSA hereby agrees to comply with all quality assurance policies, procedures, and requirements established or imposed upon QSA by PCI SSC from time to time (including but not limited to conditions and requirements imposed in connection with remediation, revocation, or any other qualification status) and that, accordingly, within 15 days of any written request by PCI SSC or any Member (each a “Requesting Organization”), except to the extent prohibited by applicable law, QSA hereby agrees to provide such Requesting Organization with such PA-DSS Assessment Results (defined below) as such Requesting Organization may reasonably request with respect to (i) if the Requesting Organization is a Member, any Vendor for which QSA has performed a PA-DSS Assessment to the extent such Vendor has provided a Payment Application to a Financial Institution of such Member, an Issuer of such Member, a Merchant authorized to accept such Member's payment cards, an Acquirer of accounts of Merchants authorized to accept such Member's payment cards or a Processor performing services for such Member's Financial Institutions, Issuers, Merchants or Acquirers or (ii) if the Requesting Organization is PCI SSC, any Vendor for which QSA has performed a PA-DSS Assessment. Each agreement between QSA and each of its Vendors (each a "Vendor Agreement") shall include such provisions as may be necessary or otherwise required by PCI SSC to ensure that QSA has all rights, licenses and other permissions necessary for QSA to comply with its obligations and requirements pursuant to this Addendum, with no conditions, qualifications, or other terms (whether in such Vendor Agreement or otherwise) that might tend to nullify, impair, or render unenforceable QSA's right to disclose such PA-DSS Assessment Results as required by this Section. Any failure of QSA to comply with this Section A.6(b) shall be deemed to be a breach of QSA's representations and warranties under the Agreement for purposes of Section A.9.3 thereof, and upon any such failure, PCI SSC may remove QSA's name from the QSA List and/or terminate this Addendum or the Agreement in its sole discretion. Additionally, QSA agrees to comply with all quality assurance standards, requirements, policies, and procedures established, mandated, or imposed upon QSA or PA-QSA Companies generally by PCI SSC from time to time, including without limitation, those relating to remediation and revocation. For purposes of the foregoing, "PA-DSS Assessment Results" means (A) all ROVs and related information, materials, and assessment results generated and/or obtained by or on behalf of QSA in connection with PA-DSS Assessments, including without limitation, all work papers, notes, and other materials or information generated or obtained in connection therewith and (B) complete and accurate copies of each Vendor Agreement; provided that such materials may be redacted in accordance with applicable PCI SSC policies and procedures, including but not limited to, redaction of pricing, delivery process, and/or confidential and proprietary information of the Vendor and/or its customers, so long as (1) such redaction is in accordance with PCI SSC policy, (2) the redacted information does not obscure any language that may tend to nullify, impair, or render unenforceable QSA's right to disclose PA-DSS Assessment Results to PCI SSC as required by this Section, and (3) upon request, QSA provides to PCI SSC a written certification that such redaction complies with the requirements of this Section executed by an executive officer of QSA.

A.7 Term and Termination

A.7.1 Term

This Addendum shall become effective as of the Addendum Effective Date and, unless earlier terminated in accordance with this Section A.7, shall continue for an initial term of one (1) year, and thereafter shall renew for additional subsequent terms of one year, subject to QSA's successful completion of qualification and re-qualification requirements for each such one-year term (each a "Contract Year"). This Addendum shall immediately terminate upon termination of the Agreement.

A.7.2 Termination by QSA

QSA may terminate this Addendum upon thirty (30) days' written notice to PCI SSC.

A.7.3 Termination by PCI SSC

PCI SSC may terminate this Addendum effective as of the end of any Contract Year by providing QSA with written notice of its intent not to renew this Addendum at least sixty (60) days prior to the end of the then-current Contract Year. Additionally, PCI SSC may immediately terminate this Addendum (i) with written notice upon QSA's breach of any representation or warranty under this Addendum; (ii) with fifteen (15) days' prior written notice following QSA's breach of any other term or provision of this Addendum (including without limitation, QSA's failure to comply with any requirement of the PA-QSA Requirements), provided such breach remains uncured when such 15-day period has elapsed, or (iii) in accordance with Section A.7.5 below.

A.7.4 Effect of Termination

Upon any termination or expiration of this Addendum: (i) QSA will no longer be identified as a PA-QSA Company on the QSA List; (ii) QSA shall immediately cease all advertising and promotion of its status as a PA-QSA Company and all references to the PA-DSS and other PCI Materials; (iii) QSA shall immediately cease soliciting for and performing PA-QSA Services (including but not limited to processing of ROVs), provided that, if and to the extent instructed by PCI SSC in writing, QSA shall complete any and all PA-QSA Services for which QSA was engaged prior to such expiration or the notice of termination; (iv) to the extent QSA is instructed to complete any PA-QSA Services pursuant to preceding clause; (iii) QSA will deliver all corresponding outstanding ROVs within the time contracted with the Vendor; (v) QSA shall remain responsible for all of the obligations, representations and warranties hereunder with respect to all ROVs submitted to PCI SSC; (vi) if requested by PCI SSC, QSA shall obtain (at QSA's sole cost and expense) the services of a replacement PA-QSA Company acceptable to PCI SSC for purposes of completing those PA-QSA Services for which QSA was engaged prior to such expiration or the notice of termination but which QSA has not been instructed to complete pursuant to clause (iii) above; (vii) QSA shall return or destroy, in accordance with the terms of Section A.6 of the Agreement, all PCI SSC and third party property and Confidential Information obtained in connection with this Addendum and the performance of PA-QSA Services; (viii) QSA shall, within fifteen (15) days of PCI SSC's written request, in a manner acceptable to PCI SSC, notify those of its Vendors with which QSA is then engaged to perform PA-DSS Assessments or other PA-QSA Services of such expiration or termination; (ix) if requested by PCI SSC, QSA shall within fifteen (15) days of such request, identify to PCI SSC in writing all Vendors with which QSA was engaged to perform PA-DSS Assessments immediately prior to such expiration or notice of termination and the status of such PA-DSS Assessments for each; and (x) notwithstanding anything to the contrary in this Addendum, the Agreement or elsewhere, PCI SSC may notify any of its Members and any Acquirers, QSA Vendors or others of such expiration or termination and the reason(s) therefor. The provisions of this Section A.7.4 shall survive the expiration or termination of this Addendum for any or no reason.

A.7.5 Revocation

(a) Without limiting the rights of PCI SSC as set forth elsewhere herein or in the Agreement, in the event that PCI SSC determines in its sole but reasonable discretion that QSA meets any condition for revocation of PA-QSA Company qualification as established by PCI SSC from time to time (satisfaction of any such condition, a "Violation"), including without limitation, any of the conditions described in Section 5.3 of the *QSA Qualification Requirements*, PCI SSC may, effective immediately upon notice of such Violation to QSA, revoke QSA's PA-QSA Company and/or Qualified Security Assessor Company qualification (each such revocation a "Revocation" for purposes of this Addendum and the Agreement), in each case, subject to reinstatement pending a successful appeal in accordance with Section A.9.5(b) of the Agreement and applicable PCI SSC policies and procedures. In the event of any Revocation: (i) QSA will be removed from the QSA List and/or such listing may be annotated as PCI SSC deems appropriate; (ii) QSA must comply with Section A.7.4 of the Addendum and Section A.9.4 of the Agreement in the manner otherwise required if the Addendum and the Agreement had been terminated; (iii) QSA will have a period of thirty (30) days from the date QSA is given notice of the corresponding Violation to submit a written request for appeal to the PCI SSC General Manager; (iv) QSA shall, within fifteen (15) days of such Revocation, in a manner acceptable to PCI SSC, notify those of its Subjects and Vendor customers with which QSA is then engaged to perform PCI DSS assessments ("PCI DSS Assessment"), PA-DSS Assessments or other Services or PA-QSA Services of such Revocation and, if applicable, of any conditions, restrictions, or requirements of such Revocation that may impact its ability to perform PCI DSS Assessments, PA-DSS Assessments or other Services or PA-QSA Services for Subjects or Vendors going forward; and (v) notwithstanding anything to the contrary in this Addendum or the Agreement, PCI SSC may notify any of its Members and any Acquirers, QSA Subjects, QSA Vendor customers, or others of such Revocation and the reason(s) therefor. In the event QSA fails to submit a request for appeal within the allotted 30-day period, this Addendum and the Agreement shall automatically terminate effective immediately as of the end of such period.

(b) All Revocation appeals proceedings will be conducted in accordance with such procedures as PCI SSC may establish from time to time; PCI SSC will review all relevant evidence submitted by QSA and each complainant (if any) in connection with therewith; and PCI SSC shall determine whether termination of any PCI SSC qualification is warranted or, in the alternative, no action, or specified remedial actions shall be required. All determinations of PCI SSC regarding Revocation and any related appeals shall be final and binding upon QSA. If PCI SSC determines that termination is warranted, then effective immediately and automatically upon such determination, this Addendum and/or the Agreement (as applicable) shall terminate, and accordingly, each corresponding PCI SSC qualification of QSA shall also terminate. If PCI SSC determines that no action is required of QSA, the Revocation shall be lifted and QSA shall be reinstated on the QSA List (as appropriate). If PCI SSC determines that remedial action is required, PCI SSC shall notify QSA and may establish a date by which such remedial action must be completed, provided that the Revocation shall not be lifted, and QSA shall not be reinstated on the QSA List, unless and until such time as QSA has completed such remedial action to the satisfaction of PCI SSC; provided that if QSA fails to complete any required remedial action by the date (if any) established by PCI SSC for completion thereof, PCI SSC may terminate this Addendum and/or the Agreement effective immediately as of such date.

A.8 General Terms

While this Addendum is in effect, the terms and conditions set forth herein shall be deemed incorporated into and a part of the Agreement, and the PA-DSS and *PA-QSA Qualification Requirements* are hereby deemed incorporated into and a part of this Addendum. This Addendum may be signed in two or more counterparts, any of which may be executed by facsimile or other form of electronic transmission acceptable to PCI SSC, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. Except as expressly modified by this Addendum or hereafter by the parties in writing, the Agreement, as modified and in effect immediately prior to the effectiveness of this Addendum, shall remain in full force and effect in accordance with its terms. This Addendum amends, restates, and supersedes in all respects each prior addendum, agreement, or understanding between the parties hereto with respect to QSA's participation in the PA-DSS Program.

Appendix B: Confirmation of PA-QSA Company's General Testing Laboratory Capabilities

The PA-QSA Company must confirm that the PA-QSA Company’s Testing Laboratory has the following capabilities using the table below, and must submit the completed form to PCI SSC along with all other required documentation in the PA-QSA Company’s application package:

A: Physical Requirements

Requirement		Findings
A1	**Requirement A1: The PA-QSA Company Testing Laboratory must have a physical address(es).**	
	Physical Location(s) of PA-QSA Company Testing Laboratory:	
A2	**Requirement A2: The PA-QSA Company Testing Laboratory must be physically secured.**	
	Describe how the PA-QSA Company Testing Laboratory is physically secured:	
A3	**Requirement A3: The PA-QSA Company Testing Laboratory must be physically restricted to authorized employees.**	
	Describe how the PA-QSA Company Testing Laboratory is physically restricted to authorized employees:	
A4	**Requirement A4: The PA-QSA Company must have implemented a quality assurance process, documented in a quality assurance manual, which includes controls for review of the PA-QSA Company Testing Laboratory’s processes and documentation and controls for the physical integrity of the PA-QSA Company Testing Laboratory’s hardware.**	
	Describe the contents of the PA-QSA Company’s quality assurance manual to confirm the procedures fully document process(es) that protect the integrity of the PA-QSA Company Testing Laboratory’s hardware:	
A5	**Requirement A5: Install all PCI DSS required security devices.**	
	List all security devices installed in the PA-QSA Company Testing Laboratory including firewalls, routers, anti-virus software, intrusion detection/prevention, and file-integrity monitoring that provide the capability of maintaining a PCI DSS compliant environment.	

Requirement	Findings
A6	**Requirement A6: Provide capabilities for penetration testing methodologies.**
	Describe the PA-QSA Company Testing Laboratory capabilities for penetration testing methodologies:
A7	**Requirement A7: Provide capabilities for forensics tools/methods.**
	Use of forensic tools/methods[1]: *Implement the capability for searching all output identified for evidence of sensitive authentication data using commercial tools, scripts, etc., per PA-DSS Requirement 1.1.1–1.1.3.*
	Describe the PA-QSA Company Testing Laboratory capabilities for forensic tools/methods:
	Describe the process for how all output will be searched:

[1] Forensic tool or method: A tool or method for uncovering, analyzing, and presenting forensic data, which provides a robust way to authenticate, search, and recover computer evidence rapidly and thoroughly. In the case of forensic tools or methods used by PA-QSAs, these tools or methods should accurately locate any sensitive authentication data written by the payment application. These tools may be commercial, open-source, or developed in-house by the PA-QSA.

B: Logical Requirements

Requirement		Findings
B1	**Requirement B1: The PA-QSA Company must assign responsibility for PA-QSA Company Testing Laboratory maintenance.**	
	Name and title of the person responsible for maintaining the PA-QSA Company Testing Laboratory:	
B2	**Requirement B2: The PA-QSA Company Testing Laboratory must be logically secured.**	
	Describe how the PA-QSA Company Testing Laboratory is logically secured—i.e., access controls:	
B3	**Requirement B3: The PA-QSA Company Testing Laboratory must be logically restricted to authorized employees.**	
	Describe how the PA-QSA Company Testing Laboratory is logically restricted to authorized employees:	
B4	**Requirement B4: The PA-QSA Company must have implemented a quality assurance process, documented in a quality assurance manual, which includes controls for review of PA-QSA Company Testing Laboratory's processes and documentation and controls for the logical integrity of the PA-QSA Company Testing Laboratory's software.**	
	Describe the contents of the PA-QSA Company's quality assurance manual to confirm the procedures fully document process(es) that logically protect the integrity of the PA-QSA Company Testing Laboratory's software:	
B5	**Requirement B5: All required security devices must be configured to be PCI DSS compliant.**	
	Configure all security devices required by PCI DSS, including: firewalls, routers, anti-virus software, intrusion detection/prevention, and file-integrity monitoring.	
	Security Device:	Briefly describe how each Security Device was configured:

Requirement		Findings

Appendix C: PA-DSS Program – Application Process Checklist

This checklist has been provided as a tool to help you organize the Payment Application Qualified Security Assessor (PA-QSA) application information that must be submitted along with your completed/signed PA-QSA Addendum. This checklist is for new PA-QSA applications only. This checklist is a tool only—please review the detailed requirements in this document to ensure completeness of submitted information.

PA-QSA Business Requirements[2]

Requirement	Information/documentation Needed
Business Legitimacy	Not applicable for PA-QSA documentation; however, this information should either: a) Already have been submitted as part original QSA application, or b) For new QSAs also applying to be a PA-QSA, included as part of QSA application per *QSA Qualification Requirements* Appendix B: Qualified Security Assessor – New Application Process Checklist.
Independence	Not applicable for PA-QSA documentation; however, this information should either: a) Already have been submitted as part original QSA application, or b) For new QSAs also applying to be a PA-QSA, included as part of QSA application per *QSA Qualification Requirements* Appendix B: Qualified Security Assessor – New Application Process Checklist.
Insurance Coverage	Not Applicable for PA-QSA documentation; however, this information should either: a) Already have been submitted as part original QSA application, or b) For new QSAs also applying to be a PA-QSA, included as part of QSA application per *QSA Qualification Requirements* Appendix B: Qualified Security Assessor – New Application Process Checklist.
Initial Processing Fee	□ Initial PA-QSA processing fee, payable to PCI SSC
PA-QSA Addendum	□ *PA-QSA Addendum* signed by company officer

[2] This checklist is for **PA-QSA Companies and Employees** and details the documentation needed to substantiate the PA-QSA Company's and Employee's qualifications to perform PA-DSS Assessments. It is also required that PA-QSA Companies and Employees be qualified as QSA Companies and Employees as well, and all PA-QSA documentation must be accompanied by QSA documentation (or that QSA documentation must be previously submitted to PCI SSC), as stated in the *Qualification Requirements for Qualified Security Assessors* document, Appendix B.

PA-QSA Company and Employee Capability Requirements[3]

Requirement	Information/documentation Needed
PA-QSA Company Services and Experience	Meet the following PA-QSA Company requirements, in addition to all QSA Requirements specified in *Qualification Requirements for Qualified Security Assessors.* ☐ Description of both relevant experience with and areas of specialization within application security and application and code reviews, preferably related to payment applications and including a description of methodology used to perform such reviews. ☐ Description of dates and clients for two previous PCI DSS Assessments performed by company ☐ Description of the PA-QSA Company's relevant areas of specialization within application security, and code reviews (for example, use of OWASP or other secure coding guidelines, web vulnerability assessment, application penetration testing, or designing or implementing cryptography systems), demonstrating at least one area of specialization. ☐ Description of cryptographic techniques, including cryptographic algorithms, key management and rotation processes, and secure key storage ☐ Description of experience using penetration testing methodologies, to include use of forensic tools/methods, ability to exploit OWASP vulnerabilities, and ability to execute arbitrary code to test processes. ☐ Two client references from recent application security assessments
PA-QSA Employee Skills and Experience	Meet the following for each PA-QSA Employee to be qualified, in addition to all QSA Requirements specified in *Qualification Requirements for Qualified Security Assessors.* For each individual applying as a PA-QSA Employee, provide a description of: ☐ Dates and clients for two previously completed PCI DSS Assessments ☐ A description of experience or work examples within secure application development, source code reviews and application testing, and cryptography with at least three (3) years of work experience, with a minimum of one year in each of the following disciplines: ☐ Ability to conduct application testing and code reviews that include but are not limited to unit, module, application, system, integration, and/or stress testing, performing web vulnerability assessments, performing application penetration testing, experience using penetration testing methodologies including the use of forensic tools/methods, and the ability to perform source code reviews.

[3] This checklist is for **PA-QSA Companies and Employees** and details the documentation needed to substantiate the PA-QSA Company's and Employee's qualifications to perform PA-DSS Assessments. It is also required that PA-QSA Companies and Employees be qualified as QSA Companies and Employees as well, and all PA-QSA documentation must be accompanied by QSA documentation (or that QSA documentation must be previously submitted to PCI SSC), as stated in the *Qualification Requirements for Qualified Security Assessors* document, Appendix B.

Requirement	Information/documentation Needed
	□ Experience in source code creation per OWASP or other secure coding guidelines, ability to exploit OWASP vulnerabilities, and ability to execute arbitrary code to test processes. □ Demonstrated competence in cryptographic techniques such as cryptographic algorithms, key management and rotation processes, and secure key storage, as determined in the sole discretion of PCI SSC.

PA-QSA Administrative Requirements[4]

Requirement	Information/documentation Needed	
PA-QSA Company's Testing Laboratory	□ Description of PA-QSA Company Testing Laboratory, using Appendix B as a template □ Inclusion of completed Appendix B: Confirmation of PA-QSA Company's General Testing Laboratory Capabilities □ Description of documented processes used by PA-QSA Company to verify vendor's testing laboratory meets the requirements specified in Appendix B, if use of vendor's testing is necessary	
PA-QSA Contact Person—Primary and Secondary	□ Name □ Title □ Address	□ Phone □ Fax □ E-mail
Background Checks	□ For each PA-QSA employee to be qualified, statement that employee successfully completed the background check in accordance with the QSA's policies and procedures □ Company Officer's signature on the *PA-QSA Addendum*	
Adherence to PCI DSS Procedures and Attestation of Validation	□ Company Officer's signature on the *PA-QSA Addendum*	

[4] This checklist is for **PA-QSA Companies and Employees** and details the documentation needed to substantiate the PA-QSA Company's and Employee's qualifications to perform PA-DSS Assessments. It is also required that PA-QSA Companies and Employees be qualified as QSA Companies and Employees as well, and all PA-QSA documentation must be accompanied by QSA documentation (or that QSA documentation must be previously submitted to PCI SSC), as stated in the *Qualification Requirements for Qualified Security Assessors* document, Appendix B.

Requirement	Information/documentation Needed
Quality Assurance	□ A description of the quality assurance procedure that will be used for PA-DSS Assessments □ A description of the responsibilities of the PA-DSS Quality Assurance contact, including at least the following: ▪ Oversight of quality assurance for all PA-DSS reports ▪ Review and approval of all PA-DSS reports prior to submission to PCI SSC ▪ Sole responsibility for submitting PA-DSS reports to PCI SSC □ A description of the contents of the PA-QSA Company's quality assurance manual to confirm the procedures fully document the PA-QSA Company's audit and report review processes for generation of the ROV using the requirements contained in the *PA-DSS Program Guide*, including at least the following: ▪ Reviews of testing procedures, reports, and supporting documentation, and other information as documented in the *PA-DSS Program Guide* related to the appropriate selection of system components. ▪ A requirement that all PA-QSA Employees must adhere to the PA-DSS. □ Company Officer's signature on the *PA-QSA Addendum*
Responsibility for QA Oversight—Primary and Secondary	□ Name □ Title □ Address □ Phone □ Fax □ E-mail
Protection of Confidential and Sensitive Information	Not applicable for PA-QSA documentation; however, this information should either: a) Already have been submitted as part original QSA application, or b) For new QSAs also applying to be a PA-QSA, included as part of QSA application per *QSA Qualification Requirements*, Appendix B – Qualified Security Assessor – New Application Process Checklist.
Evidence Retention	Not applicable for PA-QSA documentation; however, this information should either: a) Already have been submitted as part original QSA application, or b) For new QSAs also applying to be a PA-QSA, included as part of QSA application per *QSA Qualification Requirements*, Appendix B: Qualified Security Assessor – New Application Process Checklist.
Recognition of Payment Application's Validation Status	□ A statement that PA-QSA will not recognize a Payment Application's validation status until PCI SSC has notified PA-QSA and vendor via an acceptance letter and inclusion of the application on the List of Validated Payment Applications □ Company Officer's signature on the *PA-QSA Addendum*

Appendix D: Examples of Evidence

It is the expected that, for a minimum of three (3) years, PA-QSAs will secure (in accordance with Section 4.5 above) and maintain documented evidence (whether in digital or hard copy format) substantiating all conclusions in their ROVs, including but not limited to copies of any and all case logs, audit results, work papers, notes, and technical information created and/or obtained during PA-DSS Assessments. The following are examples of documented evidence acceptable for purposes of compliance with Section 4.6.

- Copies of any logs or configuration files used to validate
- Copies of any vendor written/published documentation used to validate
- Copies of any troubleshooting requests
- Any written/published vendor procedures
- Written software-development processes
- Any written process documents
- Interview Notes
- Change control documentation
- Audit logs
- System configuration files
- Written/published methodologies
- Output from any tools utilized during the assessment
- Copies/screenshots of any of the following: displays of payment card data, including but not limited to POS devices, screens, logs, and receipts
- Any document referenced mentioned as being reviewed in the ROV
- Network diagram of the lab (tested environment)
- Evidence that the applicable lab was PCI DSS compliant:
    - Firewall rules/configuration
    - IDS/IPS configuration and sensor placement
    - Antivirus solution/configuration
    - Central logging
    - Inventory of all components in lab
    - Evidence all components have latest patches
    - Evidence all components have all PCI DSS required parameters for: passwords, logging, ACLs, hardening (ports/services), etc.
- For each payment brand—e.g., Visa, MasterCard, Amex, JCB, Discover:
    - Evidence that all types of transactions were tested—e.g., approvals, different types of declines
    - Evidence that all input methods were tested—e.g., mag stripe swipe, key entry, chip& PIN
    - Evidence that all error conditions were tested—e.g., network down, acquirer/processor not responding
- *PA-DSS Implementation Guide*
- Screen shots or other hard-copy evidence from any requirement being validated by observation