Payment Card Industry (PCI)

Qualified Integrators and Resellers™

Program Guide

Version 1.1

November 2014

Document Changes

Date	Version	Description
August 2012	1.0	Initial release of the *PCI Qualified Integrators and Resellers (QIR) Program Guide*
November 2014	1.1	Minor edits to align with PCI DSS and PA-DSS v3.0

© 2012-2014 PCI Security Standards Council, LLC

Table of Contents

© 2012-2014 PCI Security Standards Council, LLC

1 Introduction

This document provides an overview of the PCI SSC Qualified Integrators and Resellers Program ("QIR Program") operated and managed by PCI Security Standards Council, LLC ("PCI SSC"), and should be read in conjunction with the *QIR Qualification Requirements*, and the other documents referenced in Section 1.2 below. This document describes the following:

- QIR Program Background
- QIR Program Roles and Responsibilities
- QIR Program Overview
- Pre-Implementation Activities
- Qualified Installation Process Overview
- Post-Implementation Activities
- QIR Company Quality Assurance Program

1.1 QIR Program Background

.

PCI SSC operates the Payment Application Data Security Standards (PA-DSS) program. The program promotes the development and implementation of secure commercial payment applications that do not store prohibited data, and helps to ensure that payment applications support compliance with the PCI DSS.

Organizations qualified by PCI SSC to implement, configure, and/or support validated PA-DSS Payment Applications on behalf of merchants and service providers are referred to as "Qualified Integrator and Reseller Companies" or "QIR Companies," The quality, reliability, and consistency of a QIR Company's work provide confidence that the application has been implemented in a manner that supports the customer's PCI DSS compliance.

1.2 Related Publications

The *Payment Card Industry (PCI) Qualified Integrators and Resellers (QIR) Program Guide* (or *"QIR Program Guide"*) should be used in conjunction with the latest versions of the following other PCI SSC publications, each as available through the Website:

- *QIR Qualification Requirements,* which defines requirements that must be satisfied by all QIR Companies in order to perform Qualified Installations
- PCI DSS, which sets the foundation for other PCI Standards and related requirements
- PA-DSS, which defines the specific technical requirements and provides related assessment procedures and templates used to validate payment applications and document the validation process

1.3 Terminology

Except as otherwise specified herein, capitalized terms used but not defined in this document shall have the meanings ascribed to them in *Schedule 1* to the then current version of the *PCI Qualified Integrator and Reseller (QIR) Agreement* (the "*QIR Agreement*"). The *QIR Agreement* is attached as *Appendix A* to the then most current version of the *QIR Qualification Requirements*.

© 2012-2014 PCI Security Standards Council, LLC

1.4 QIR Program Role and Responsibilities

The QIR Program simplifies the process for identifying and engaging integrators and resellers qualified to assist merchants and industry participants in their effort to install validated PA-DSS payment applications in a manner that facilitates PCI DSS compliance.

QIR Company may be any form of legal entity and must comply with all QIR Company Requirements.

Only QIR Companies that are in "Good Standing" as QIR Companies are permitted to perform Qualified Installations. All QIR Companies are listed on the QIR List.

QIR Company responsibilities generally include (without limitation) the following:

- Ensuring installations and configuration of validated PA-DSS Payment Applications are in accordance with the applicable *PA-DSS Implementation Guide* in a manner which supports PCI DSS compliance.
- Providing the customer with a completed *QIR Implementation Statement* after installation and configuration of a validated PA-DSS application.
- Documenting, in the *QIR Implementation Statement*, for the customer any potential risks to PCI DSS compliance the QIR Employee might identify in the due course of installing, configuring, or maintaining the validated PA-DSS payment application.
- Maintaining a quality assurance program that includes vetting of employees involved in Qualified Installations, personnel training, and education on PCI DSS and applicable *PA-DSS Implementation Guides.*
- Protection of confidential and sensitive information.
- Supporting any PFI forensic investigations in which the application the QIR Company installed at a customer environment may be involved.
- Servicing the payment applications (for example, troubleshooting, delivering remote updates, and providing remote support) if engaged to do so, according to the *PA-DSS Implementation Guide* and PCI DSS.

© 2012-2014 PCI Security Standards Council, LLC

2 Program Overview

The goal of the QIR Program is to educate, qualify, and train organizations involved in the implementation, configuration, and/or support of a validated PA-DSS payment application on behalf of a merchant or service provider. The program focuses on two core objectives:

- Ensuring that QIR Companies install and configure validated PA-DSS payment applications into customer environments in a manner that supports PCI DSS compliance, and
- Ensuring that QIR Companies are accountable for ensuring that such installations facilitate their customers' PCI DSS compliance efforts.

2.1 Fees

Fees to participate as a QIR Company in the QIR Program are specified in the *QIR Program Fee Schedule* on the Website.

Pricing and fees charged by QIR Companies for the services they provide to customers in connection with Qualified Installations are negotiated directly between the QIR Company and the applicable customer. Fees and pricing for Qualified Installations and related services of QIR Companies are not set by PCI SSC, and PCI SSC is not involved in any way with such fees or pricing.

2.2 QIR Approval Process

In an effort to help ensure that each QIR Company and QIR Employee possesses the requisite knowledge, skills, experience, and capacity to perform installations of validated PA-DSS applications in a proficient manner and in accordance with industry expectations, companies and individuals desiring to perform Qualified Installations must first be approved as QIR Companies or QIR Employees (as applicable), and then must maintain that approval in Good Standing.

Please refer to the *QIR Qualification Requirements* to review specific information regarding qualification as a QIR Company or QIR Employee.

2.3 QIR Required Requalification Processes

In addition to all other applicable requirements, each QIR Company must perform the processes listed below in order to remain in Good Standing every three years:

- Re-qualify (applies to QIR Companies and QIR Employees).
- Attend training provided by PCI SSC, and legitimately pass, of his or her own accord without any unauthorized assistance, all required QIR Program training examinations (applies to QIR Employees only). QIR Employees who fail any such exams must pass the exams before they lead or manage any Qualified Installation.
- Annually review and update, as applicable, the QIR Company's Quality Assurance manual (applies to QIR Companies and QIR Employees).
- Annually renew and review PA-DSS application training materials to maintain current knowledge of all major and minor software changes (applies to QIR Companies and QIR Employees).
- Train employees and contractors with access to customer sites on how to access, install, maintain and support payment applications (and any connected systems) in accordance with the information provided by the application vendor in the *PA-DSS Implementation Guide* and other supporting materials (applies to QIR Companies only).

© 2012-2014 PCI Security Standards Council, LLC

3 Pre-Implementation Activities

3.1 Preparation

To help ensure that each QIR Company and QIR Employee possesses the requisite knowledge, skills, experience, and capacity to perform Qualified Installations in a proficient manner, and in accordance with industry expectations, each QIR Company and each QIR Employee is required at all times to satisfy all applicable *QIR Qualification Requirements*. The current version of these requirements is available on the Website.

Applications validated as compliant with the PA-DSS and accepted by PCI SSC are identified on the list of validated Payment Applications on the Website (the "Application List"). Only the specific versions of the Payment Applications that appear in the Application List ("Validated Application Versions") have been evaluated and determined to comply with the PA-DSS and therefore are eligible for Qualified Installations.

Preparation activities that the QIR Company must consider prior to undertaking a Qualified Installation include but are not limited to:

- Sell and install only those Validated Application Versions that are identified on the Website as "Acceptable for New Deployments."
    - Confirm before the start of a new Engagement that the application is Acceptable for New Deployments.

There are two types of Validated Payment Applications: "Acceptable for New Deployments" and "Acceptable only for Pre-Existing Deployments." These are identified as two different tabs on the Website and also in the Deployment Notes for each validated application.

- Be prepared to answer any questions the customer may have, or know where to refer the customer, regarding the payment application listing information on the Website, such as:
    - The Revalidation Date is based on the acceptance of a specific application by PCI SSC. Each validated payment application must undergo an annual attestation until the Expiry Date is reached. Payment applications that have not yet expired appear on the Acceptable for New Deployments list.

The annual attestation process has been adopted to encourage software vendors to not only reaffirm that there have been no updates to the PA-DSS Validated Payment Application (if applicable), but also to encourage vendors to periodically consider whether updates to the PA-DSS Validated Payment Application are necessary to address changes to the external threat environment in which the payment application operates.

© 2012-2014 PCI Security Standards Council, LLC

- The Expiry Date is based on the lifecycle of PA-DSS. All payment applications validated to a particular version of PA-DSS expire on the same date. When the Expiry Date is reached, if a specific payment application has not been validated against the then-current version of PA-DSS, it will be placed on the Acceptable only for Pre-Existing Deployments list.
- The operating system(s) on which the PA-DSS application has been tested and any dependent hardware or software requirements are listed for each payment application on the Website. It is the responsibility of the QIR Company and applicable QIR Employee to ensure that the customer's environment meets these minimum requirements for each payment applications' implementation.
- Notify the customer that PCI DSS compliance is at risk if any application they choose to install or maintain has been identified as vulnerable or does not appear on the Application List as Acceptable for New Deployments.

- Ensure that all new and existing QIR Employees and contractors who have access to customer sites, cardholder data or a customer's CDE (cardholder data environment) meet the requirements of PCI DSS 12.7.

PCI DSS 12.7 *Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)*

- The QIR Employee should, prior to undertaking a Qualified Installation, review the latest payment application vendor instructional documentation, *PA-DSS Implementation Guide* and training programs for the specific version of the validated PA-DSS application.
- Provide the customer with the name of the Lead QIR who will be responsible for the Engagement and their role and responsibility, an estimate of work to be performed, expected duration of the work, and notice of any potential down time.
- Provide the customer with a copy of the QIR Feedback Form, or link to the Website where the form can be filled out and submitted to PCI SSC.
- Determine the level of access that will be required to and/or at the customer site, and strictly follow secure access, installation, maintenance, and support processes outlined in the application vendor's latest *PA-DSS Implementation Guide*.
- Ensure that QIR Employee access credentials are unique per QIR Employee and per customer.
- Develop an installation, configuration, and maintenance plan from the information provided by the application vendor in the *PA-DSS Implementation Guide* and any other supporting materials.

© 2012-2014 PCI Security Standards Council, LLC

4 Qualified Installation Process Overview

4.1 Implementation Execution

The *PA-DSS Implementation Guide* is provided by the vendor of the validated payment application and is used by the QIR Company to install, configure, and maintain the payment application. Any questions about this document should be directed to the application vendor.

The *QIR Implementation Statement* provides a checklist of tasks to be completed as part of a Qualified Installation. Some or all of these tasks will apply to any given implementation. It is the responsibility of the Lead QIR to understand how each item within the *QIR Implementation Statement* applies to the particular implementation.

All tasks in the *QIR Implementation Statement* are the responsibility of the Lead QIR. Some of the tasks may be automatically performed by the payment application. Other tasks will be performed by the QIR Employee; the *PA-DSS Implementation Guide* for the validated payment application will provide instructions on how to configure the payment application or other software. The customer may prefer to perform some tasks themselves. It is important that the Lead QIR document all tasks that both the QIR Company and customer are going to perform, and that both the QIR Company and their customer understand and agree to the tasks before commencement.

The *QIR Implementation Statement* and the *PA-DSS Implementation Guide* must both be used during the installation. The QIR Company must retain evidence of all configurable elements of a Qualified Installation (whether performed by the QIR Employee or customer) and must retain these work papers as part of the installation documentation. Examples of types of evidence are provided in Appendix A.

© 2012-2014 PCI Security Standards Council, LLC

5 Post-Implementation Activities

5.1 Implementation Reporting

The *QIR Implementation Statement* must be produced as part of each Engagement and must be completed and delivered to the customer no later than ten (10) business days after completion of the Qualified Installation.

A template for the *QIR Implementation Statement* is available on the Website, together with supporting guidance (in the *QIR Implementation Instructions*) on how the *QIR Implementation Statement* should be completed. QIR Companies must follow the defined format for all Qualified Installations.

The following information must be included in the *QIR Implementation Statement*:

- Customer's company and contact details
- Name of QIR Company
- Name and contact details of the Lead QIR
- Name and contact details of the QIR Employee who completes the peer review, and
- PA-DSS Validated Payment Application name, version number and reference number as shown on the Website

Requested Content	Explanation
Peer Review	The *QIR Implementation Statement* must be reviewed by a second QIR Employee to confirm accuracy and completeness. The QIR Employee completing the review must sign the *QIR Implementation Statement*.
Signatures	The signature of the Lead QIR and QIR Employee completing the peer review indicates acceptance of responsibility and accountability for the completed installation. The signature of the customer is required to confirm a copy of the *QIR Implementation Statement* has been provided to them. The Lead QIR is expected to review the results of the installation with the customer to demonstrate the Payment Application has been installed and configured in a manner that supports compliance with PCI DSS; and if applicable, that potential areas of vulnerability have been identified.

The *QIR Implementation Statement* "Details" section contains a list of tasks that must be performed by the QIR Employee during the Qualified Installation. The activities conducted during the installation and configuration of the Payment Application must be recorded so that the customer understands, and has a record of, changes made to their environment. The *QIR Implementation Instructions* provides details for each task. If an activity is not or cannot be performed, for example, the customer will be executing the task rather than the QIR Employee, it must be noted in Part 3 of the *QIR Implementation Statement*, as "QIR Additional Observations."

© 2012-2014 PCI Security Standards Council, LLC

The QIR Additional Observations section is where the QIR Employee should note any observations or details applicable to the overall installation that the customer needs to be aware. Any anomalies or issues observed that may affect the customers' PCI DSS compliance should be recorded. The QIR Additional Observations section must also record explanations for any tasks that could not be or were not performed as part of the Qualified Installation.

The QIR Company must store the *QIR Implementation Statement* and any associated work papers must be retained in accordance with the QIR Company's current evidence retention policy and procedures for a minimum of three (3) years from the completion of the Qualified Installation. PCI SSC reserves the right to examine these documents upon reasonable notice as part of the quality assurance process.

At the end of the Qualified Installation, the QIR Employee should encourage the customer to complete and return the QIR Feedback Form to PCI SSC. Customer feedback is essential to the QIR Quality Assurance Program (further described in Section 7 below) to highlight project success and learn from project history. QIR Companies are required to inform customers that the latest version of the QIR Feedback Form can be found on the Website.

5.2 Ongoing Support

The QIR Company may be asked to manage the payment application after installation. This may include applying updates or patches, changing configurations, etc. Work must be conducted in accordance with the *PA-DSS Implementation Guide* and the *QIR Implementation Statement*.

When debugging or troubleshooting for customers, the QIR Company must verify that any cardholder data, if necessary to resolve a problem, is collected in limited amounts, encrypted while stored, and securely deleted immediately after use.

The QIR Company must immediately report all vulnerabilities or potential breaches to the customer.

The QIR Company must review, at least annually, updates to the applicable *PA-DSS Implementation Guide* and supporting documentation to remain current with all major and minor software changes, and QIR Company training materials must be updated to reflect all major and minor software changes.

5.2.1 Remote Access

If support is being provided remotely, the QIR Company must:

- Advise customers to turn on remote management only when necessary, monitor when in use, and to turn off access immediately thereafter.
- Use remote management software only when absolutely necessary, and in a secure manner, to access customer sites for the purposes of installation, support, and maintenance.
- Use two-factor authentication with strong cryptography.

QIR Companies using remote access software must follow the *PA-DSS Implementation Guide*, which contains instructions on using remote access security features. The QIR Company is required to manage all remote access to customers as follows:

- Site access must be restricted and authentication credentials assigned to only those personnel who need access.

© 2012-2014 PCI Security Standards Council, LLC

- Remote QIR Company access to customer sites must only come from specific and known IP addresses.
- Unique, complex and secure authentication credentials must be used for each customer.
- Data transmissions must always be encrypted.

5.2.2 PFI Support

If the QIR Company is asked to participate in the investigation of a breach at the customer environment where the QIR Company installed a validated PA-DSS payment application, the QIR Employee may be requested to provide copies of the *QIR Implementation Statement* and associated documentation from the Engagement to the customer or to the applicable PCI SSC-qualified PCI Forensic Investigator (PFI), and must cooperate with all such requests. A list of PFIs appears on the Website.

5.3 Engagement Termination

When an Engagement ends, the QIR Company must perform clean-up tasks that include but are not limited to:

- Ensuring credentials are securely removed from all customer sites after any installation or maintenance tasks have been completed.
- Providing instructions for the customer to remove QIR Company user accounts and credentials, if the QIR Company no longer supports the customer.
- Providing instructions for the customer to eliminate all connectivity—for example, open firewall ports—between the QIR Company and the customer.

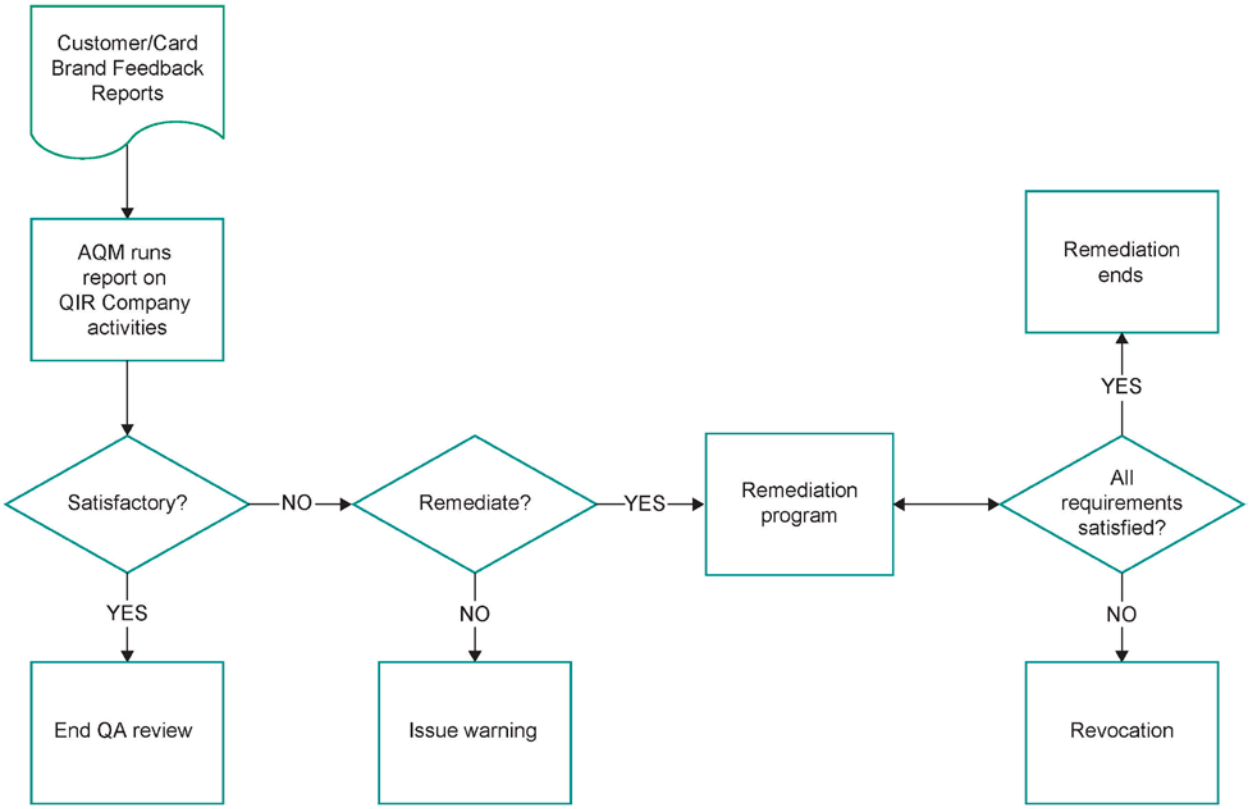
© 2012-2014 PCI Security Standards Council, LLC

6 QIR Quality Assurance Program

QIR Companies are required to meet all quality assurance (QA) requirements set by PCI SSC. As part of the QIR Program, PCI SSC operates its QIR Quality Assurance Program through its Assessor Quality Management team (AQM) to ensure that QIR Companies and QIR Employees comply with the *QIR Qualification Requirements*, the *QIR Program Guide* and with the QIR Company's own documented processes and procedures for Qualified Installations.

6.1 PCI SSC Responsibilities

PCI SSC collects feedback on QIR Company performance from QIR Company customers, payment card brands, and others. This feedback is assessed to determine whether the QIR Company's performance is meeting the expected quality levels. So long as PCI SSC determines in its reasonable discretion that a QIR Company continues to satisfy applicable QIR Requirements and meets prescribed quality levels for Qualified Installations, that QIR Company will remain in Good Standing as a QIR Company. Failure to satisfy applicable requirements or meet applicable quality levels may result in any or all of the actions described in Section 6.3 below.



© 2012-2014 PCI Security Standards Council, LLC

6.2 QIR Company Responsibilities

The QIR Company is expected to manage an internal quality assurance program that meets the expectations of PCI SSC. The QIR Company's Quality Assurance manual, which describes the QIR Company's internal quality assurance program, must be reviewed and updated annually. PCI SSC reserves the right to request and review this manual upon reasonable notice. The Quality Assurance manual must include:

- Procedures requiring all QIR Employees and contractors with access to customer sites to strictly follow secure access, installation, maintenance, and support processes outlined in the application vendor's latest *PA-DSS Implementation Guide*
- Appropriate requirements, processes, and procedures regarding reviews of performed installation procedures, supporting documentation, and information documented in *QIR Implementation Statements* relating to installation recommendations; and thorough documentation of all installation results
- A requirement for peer review of all *QIR Implementation Statements* (a second QIR Employee must countersign the *QIR Implementation Statement* of the Lead QIR)
- A requirement that all QIR Employees must adhere to the *QIR Program Guide* and all QIR Employee Requirements
- A requirement for documentation of disciplinary action if an employee or contractor fails to securely access, install, maintain, or support payment applications (and any connected systems) in accordance with industry data security best practices and standards
- Procedures for retention of training records to confirm that all QIR Employees, before being assigned to a Qualified Installation, have received training in accordance with Requirement 3.1.1 of this document

The QIR Company must notify PCI SSC and take appropriate steps to remain a QIR Company in Good Standing should the number of QIR Employees drop below two (2). If the minimum number of QIR Employees is not maintained, the QIR Company may be removed from the QIR List until this requirement is satisfied. A grace period of thirty (30) days is granted to enable QIR Companies that drop below two (2) QIR Employees to meet this requirement. If the number of QIR Employees drops below two, the QIR Company may continue to perform Qualified Installations only if contracted with another QIR Company for the peer review. If, at the end of the thirty (30) days, the QIR Company does not meet the minimum requirements, the QIR Company may be removed from the QIR List and become ineligible to perform new Qualified Installations until such time as the minimum requirement is satisfied.

6.3 Feedback Process

Following each Qualified Installation, the QIR Company must request that the customer submit to PCI SSC a QIR Feedback Form, which can be found on the Website.

Any payment card brand, acquiring bank, and other person or entity may submit to PCI SSC a completed QIR Feedback Form for a QIR Company that completed a Qualified Installation. Additionally, a Qualified Security Assessor (QSA) that assesses a merchant or service provider that has had a Qualified Installation performed may submit a QIR Feedback Form regarding the QIR Company that performed that installation.

The QIR Feedback Form addresses the following:

- Adequacy of *QIR Implementation Statement* content;

© 2012-2014 PCI Security Standards Council, LLC

- Competence of staff assigned to Qualified Installation Engagements;
- Ability to effectively communicate the results of the Qualified Installation and any potential risks or exposures identified during the Qualified Installation.

6.3.1 Warnings

PCI SSC may issue warnings to QIR Companies who fail to meet applicable QIR Requirements or demonstrate a need for improvement in one or more areas of their Qualified Installations. When PCI SSC issues a warning, the QIR Company will be monitored. Monitoring by PCI SSC can include:

- Review of QIR Feedback Forms,
- Review of Qualified Installation materials, and/or
- On-site reviews of Qualified Installations, for which expenses must be paid by the QIR Company.

When PCI SSC has determined that quality has sufficiently improved, the QIR Company will be returned to Good Standing. Two consecutive warnings may result in remediation. Qualified Installations may continue to be performed after receiving a warning, subject to the terms of remediation (if applicable) and potential revocation.

6.3.2 Remediation

If the QIR Company fails to meet applicable QIR Requirements, the quality of Qualified Installations otherwise becomes unsatisfactory, or moderate deficiencies have not been resolved after prior warning, PCI SSC reserves the right to require the QIR Company to enter into remediation. Prior warning is not a prerequisite for remediation.

- Upon being identified for remediation, PCI SSC will issue a remediation notice and the QIR Company's status will change from Good Standing to In Remediation on the QIR List.
- QIR Employees may be required to retake all training and pass any associated examination within 30 days of the remediation notice.
- QIR Companies may be required to permit PCI SSC and/or its representatives to visit and audit the QIR Company's offices, facilities, books, and records relating to the QIR Company's Quality Assurance program, in each case at the expense of the QIR Company. During remediation, QIR Companies are permitted to perform Qualified Installations.
- Failure to comply with required remediation requirements, processes, or procedures will result in immediate revocation of QIR Company qualification and removal from the QIR List.
- If PCI SSC determines that the QIR Company meets all applicable requirements and quality standards during remediation, remediation will cease and the QIR Company's status will return to In Good Standing. If PCI SSC determines that the QIR Company fails to meet applicable QIR requirements or quality standards in connection with remediation, QIR Company status will be revoked.
- PCI SSC reserves the right at all times to annotate the QIR Company's listing on the QIR List to indicate the QIR Company's current status and related information, including but not limited to whether the QIR Company is in remediation.

© 2012-2014 PCI Security Standards Council, LLC

6.3.3 Revocation

If a QIR Company fails to meet applicable QIR Requirements (including but not limited to required QIR Quality Assurance Program quality levels), QIR Company status may be revoked. Upon revocation, the company will be removed from the QIR List, subject to reinstatement pending a successful appeal in accordance with the *QIR Agreement*, and/or termination of the *QIR Agreement*. Prior warning and/or remediation are not prerequisites for revocation.

Each of the following conditions constitutes a "Violation" for purposes of the *QIR Agreement*, which may result in immediate Revocation (defined in the *QIR Agreement*), including removal from the QIR List:

- The QIR Company (or any QIR Employee thereof) violates any obligation regarding non-disclosure of confidential materials.
- The QIR Company (or any QIR Employee thereof) fails to maintain physical, electronic, and procedural safeguards to protect confidential or sensitive information; and/or fails to report to PCI SSC unauthorized access to any system that stores confidential or sensitive information.
- The QIR Company (or any QIR Employee thereof) engages in unprofessional or unethical business conduct, including misrepresentation of the PCI DSS or any other PCI SSC requirements or documents to sell products or services.
- The QIR Company (or any QIR Employee thereof) fails to provide quality services, based on customer feedback or evaluation by PCI SSC, any of its affiliates or any third party.
- The QIR Company (or any QIR Employee thereof) is determined to have cheated on any exam in connection with QIR training, including without limitation, submitting work that is not the work of the QIR Employee taking the exam; theft of or unauthorized access to an exam; use of an alternate, stand-in, or proxy during an exam; use of any prohibited or unauthorized materials, notes, or computer programs during an exam; and providing or communicating in any way any unauthorized information to another person during an exam.
- The QIR Company (or any QIR Employee thereof) is determined by PCI SSC to have provided false or intentionally incomplete or misleading information to PCI SSC in any application or other materials.
- The QIR Company (or any QIR Employee thereof) permits any unqualified professional to perform (or participate in the performance of) any Qualified Installation for or on behalf of such QIR Company.
- The QIR Company is otherwise not in Good Standing.
- The QIR Company (or any QIR Employee thereof) fails to perform any Qualified Installation in accordance with the *QIR Program Guide*.
- Forensic evidence reveals that a security or data breach of the QIR Company led to a security or data breach of any of the QIR Company's Qualified Installation customer.
- The QIR Company fails to provide proof of Continuing Professional Education (CPE) hours for its QIR Employees The QIR Company (or any QIR Employee thereof) fails to promptly notify PCI SSC of any event described above that

© 2012-2014 PCI Security Standards Council, LLC

occurred less than two (2) years before such QIR Company's or QIR Employee's qualification by PCI SSC.

If QIR Company status is revoked, the QIR Company will be removed from the QIR List and is no longer recognized by PCI SSC as approved to perform Qualified Installations. QIR Companies may appeal revocation but must meet all applicable QIR Requirements, including without limitation, all applicable remediation requirements, in order to regain Good Standing as a QIR Company.

All appeals must be submitted to PCI SSC in writing within thirty (30) days of revocation, addressed to the PCI SSC General Manager, and must follow all applicable procedures as specified by PCI SSC. PCI SSC will review all relevant information submitted in connection with such appeals, and all decisions of PCI SSC regarding revocation on appeal are final.

Upon revocation, 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) after the date of revocation or unsuccessful resolution of appeal, whichever is later. When QIR Company status has been revoked, a QIR Company is not permitted to complete pending Engagements or Qualified Installations unless instructed by PCI SSC in writing.

6.4 QIR Audits

As part of the QIR Quality Assurance Program process, PCI SSC reserves the right to conduct QIR Company site/facility audits for purposes of assessing whether the processes and procedures used by the QIR Company for Qualified Installations comply with applicable QIR Program requirements, including but not limited to review of related books, records, and other work product for such purpose; and each QIR Company must provide PCI SSC with reasonable access to such site/facility, books, records, and other work product for such purposes.

For quality assurance purposes, the QIR Company may redact sensitive or confidential information that does not materially impact the review.

© 2012-2014 PCI Security Standards Council, LLC

Appendix A: Acceptable Forms of Documented Evidence

For a minimum of three (3) years, QIR Companies must secure and maintain documented evidence (whether in digital or hard copy format) substantiating all services, including but not limited to copies of any and all case logs, configuration and other installation results, work papers, notes and technical information created and/or obtained during each Qualified Installation.

The following forms of documented evidence are acceptable for purposes of compliance with *QIR Program Guide.*

- Copies of any logs or configuration files used or generated
- Copies of any application-vendor written/published documentation used
- Copies of any troubleshooting requests raised with the application vendor during or as a result of the implementation
- Any written/published application-vendor procedures used during the implementation
- Any written process documents
- Interview notes
- Change-control documentation
- Installation logs
- System-configuration files
- Written/published methodologies
- Any written/published vendor procedures
- Copies/screenshots of any of the following: displays of payment card data including but not limited to POS devices, screens, logs, and receipts
- Screenshots of any configuration settings including but not limited to those settings relevant to secure authentication, logging, and remote access

© 2012-2014 PCI Security Standards Council, LLC