![PCI Security Standards Council logo]

Payment Card Industry (PCI)

Qualified Integrator and Reseller (QIR)™

Program Guide
Version 4.0

March 2018

Document Changes

Date	Version	Description
August 2012	1.0	Initial release of the *PCI Qualified Integrators and Resellers (QIR) Program Guide*
October 2014	1.1	Minor edits to align with PCI DSS and PA-DSS v3.0
N/A	2.0	Version number not used
September 2015	3.0	Minor edits to simplify program, e.g., Allowing sole proprietors to join the program by removing the requirement to have two trained employees on staff at all times
March 2018	4.0	Update to reflect QIR Program Expansion

QIR Program Guide, v 4.0
© 2018 PCI Security Standards Council, LLC
March 2018
Page i

904717.1
962665.3

Contents

1 Introduction

This document provides an overview of the PCI SSC Qualified Integrator and Reseller (QIR)™ Program ("QIR Program") operated and managed by PCI Security Standards Council, LLC ("PCI SSC"), and should be read in conjunction with the *Payment Card Industry (PCI) Qualified Integrator and Reseller (QIR)™ Qualification Requirements* ("QIR Qualification Requirements"), and the other documents referenced in Section 1.2 below. Capitalized terms used but not otherwise defined herein are defined in Schedule 1 to the *QIR Qualification Requirements*. This document describes the following:

- QIR Program Overview
- QIR Program Roles and Responsibilities
- Qualified Installation Process Overview
- QIR Quality Management

1.1 QIR Program Overview

The QIR Program offers a credential (the QIR Professional Qualification) for those industry practitioners who implement, configure, and/or support Payment Applications and related payment technologies and services on behalf of merchants and service providers. To gain the qualification, the practitioner must demonstrate their knowledge of those critical security controls that mitigate the most common causes of loss of Cardholder Data in the payment card industry today.

QIR Professional Qualification provides confidence in the quality, reliability, and consistency of a QIR Professional's work and that the Payment Application and related technologies they install, configure, and service have been implemented in a manner that targets the Customer's security risk.

The QIR Program also simplifies the process for identifying and engaging integrators and resellers qualified by PCI SSC to assist merchants and service providers in their efforts to install Payment Applications and related technologies in a manner that targets security risk.

A QIR Professional may be anything from an independent contractor working in a legal structure appropriate for the region in which they operate, to an employee of an organization engaged in implementing, configuring, and/or supporting Payment Applications and related technologies on behalf of merchants and service providers.

Only those individuals who are qualified by PCI SSC and are in "Good Standing" (or in compliance with the terms of Remediation, defined in Section 5.2 below) as QIR Professionals are permitted to perform Qualified Installations. All QIR Professionals are identified on the QIR List on the Website.

Note: PCI SSC also operates the Payment Application Data Security Standard (PA-DSS) Program. The PA-DSS 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. When implementing, configuring, or supporting PA-DSS Validated Payment Applications, QIR Professionals reference the PA-DSS Program material on the Website, which includes a list of Validated Payment Applications. There is provision in the QIR Implementation Statement to record relevant details about PA-DSS Validated Payment Applications.

904717.1
962665.3

1.2 Related Publications

This *Payment Card Industry (PCI) Qualified Integrator and Reseller (QIR)*^{TM} *Program Guide* (the "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 QIR Professionals in order to perform Qualified Installations

- ▪ ***PCI DSS,*** which sets the foundation for other PCI SSC standards and related requirements

- ▪ ***PA-DSS,*** which defines the specific technical requirements and provides related assessment procedures and templates used to validate eligible Payment Applications and document the validation process

- ▪ ***QIR Implementation Statement,*** which is a template used to document the results of a Qualified Installation

- ▪ ***QIR Implementation Instructions,*** which is a guidance document used to explain how to complete the *QIR Implementation Statement*

904717.1
962665.3

2 Program Responsibilities

2.1 General Responsibilities

A QIR Professional's responsibilities generally include (without limitation) the following:

- Ensuring that the installation or upgrade of Payment Applications and related technologies· and provision of related services and activities in connection with the deployment, configuration, or access to any of the customer's foregoing· in a Customer's Cardholder Data environment is implemented in a manner that addresses high-priority security risks

- Providing the Customer with a completed *QIR Implementation Statement* after completion of a Qualified Installation

- Documenting any potential security risks identified by the QIR Professional in the *QIR Implementation Statement*

- Protecting confidential and sensitive information

- Supporting any investigations by PCI Forensic Investigators relating to Customers and/or Cardholder Data environments with respect to which the QIR Professional performed any Services in connection with the QIR Program

- Servicing the Payment Applications and related technologies· for example, troubleshooting, delivering remote updates, and providing remote support· if engaged to do so, in accordance with the information provided by the application vendor in implementation or installation guidance or other relevant supporting materials, and in accordance with PCI DSS

2.2 QIR Program Objectives

The QIR program focuses on the following objectives:

- Reducing the likelihood of Cardholder Data loss from merchant or service provider payment environments resulting from faulty Payment Application or related technology installations

- Providing education to help prepare QIR Professionals to install and configure Payment Applications and related technologies into Customer environments in a manner that addresses high-priority security risks

To help achieve these program objectives, PCI SSC requires all QIR Professionals to requalify annually (including successful completion of requalification exams) to maintain their qualification in Good Standing and lead or manage Qualified Installations.

Please refer to the *QIR Qualification Requirements* to review specific information regarding requalification as a QIR Professional, or for more information on initial application and qualification processes.

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

904717.1
962665.3

3 Qualified Installation Process Overview

3.1 Pre-Implementation Activities

3.1.1 Preparation

In order to demonstrate the requisite knowledge, skills, experience, and capacity to be qualified by PCI SSC to perform Qualified Installations, each QIR Professional is required to satisfy all requirements and submit all materials specified in the *QIR Qualification Requirements*. The current version of the *QIR Qualification Requirements* is available on the Website.

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

- Verifying that the Customer's environment meets the minimum requirements for software or hardware for the payment technologies that are included in Qualified Installation.

- Confirming that all QIR Professionals working on the QIR Installation meet the requirements of PCI DSS 12.7, which states: *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.)*

- Reviewing the latest vendor documentation and training programs available for the specific version(s) of the Payment Application and/or related technologies involved, prior to undertaking a Qualified Installation

- Providing the Customer with the name of the QIR Professional who will be responsible for the Engagement, an estimate of work to be performed, expected duration of the work, and notice of any potential down time

- Directing the Customer to the *QIR Feedback Form for Payment Brands and Others* ("QIR Feedback form") on the Website, where the form can be completed and submitted to PCI SSC

- Determining the level of access required to support the Customer, and strictly following secure access, installation, maintenance, and support processes outlined in the payment technology vendor's latest installation or implementation guidance

- Ensuring that QIR Professional access credentials are unique per QIR Professional and per Customer

- Notifying the Customer that security is at risk if any application or other technology they choose to install or maintain has been identified as vulnerable

- Developing an installation, configuration, and maintenance plan from the information provided by the payment technology vendor in the vendor's installation or implementation guidance

3.1.2 Implementation Execution

QIR Professionals should refer to vendor documentation such as Implementation Guides (required for PA-DSS Validated Payment Applications), installation instructions, and other supporting materials to install, configure, and maintain the Payment Application and other payment technologies. Any questions about such documentation should be directed to the 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 QIR Professional 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 QIR Professional. Some of the tasks may be automatically performed by the Payment Application or other payment technologies, while the QIR Professional will perform other tasks. The Customer may choose to perform some of these tasks rather than the QIR Professional. It is important that the QIR Professional document all tasks that both they and the Customer are to perform, and that both the QIR Professional and the Customer understand and agree to the tasks before starting.

Both the *QIR Implementation Statement* and the vendor documentation for the payment technologies must be used during the installation. The QIR Professional must retain evidence of all configurable elements of a Qualified Installation (whether performed by the QIR Professional or Customer) and must retain these work papers as part of the installation documentation. Examples of types of evidence are provided in Appendix A.

3.2 Post-Implementation Activities

3.2.1 Implementation Reporting

When performing a Qualified Installation, the QIR Professional is required to complete a *QIR Implementation Statement* in accordance with the *QIR Implementation Instructions*.

The *QIR Implementation Statement* confirms what the QIR Professional did, what they observed, and what they informed the Customer of in connection with the Qualified Installation. The QIR Professional is not performing a PCI DSS assessment. Compliance with PCI DSS remains the responsibility of the Customer.

A *QIR Implementation Statement* must be produced as part of each Qualified Installation and must be delivered to the Customer within ten (10) business days after completion of the Qualified Installation.

Note: There may be multiple retail locations, corporate offices, or other places where applications or related technologies are installed as part of the Qualified Installation. Where a Qualified Installation involves multiple customer locations, the QIR Professional may choose to prepare a number of QIR Implementation Statements that together represent all locations.

The QIR Professional must store the *QIR Implementation Statement* and any associated work papers 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 its quality assurance process.

A template for the *QIR Implementation Statement* is available on the Website. Supporting guidance, the *QIR Implementation Instructions*, is also on the Website and explains how to complete the *QIR Implementation Statement*.

The *QIR Implementation Statement* has three (3) parts, and QIR Professionals must follow the defined format for all Qualified Installations:

Part 1: Implementation Statement Summary	Records details about the QIR Professional and the services provided in connection with the Qualified Installation, whether onsite or remotely. Includes required signatures for the Customer acknowledgment and the QIR Professional's affirmation of the Qualified Installation.
Part 2: Implementation Statement Details	Records details about the activities performed by the QIR Professional during the Qualified Installation. This part is divided into two sections: Part 2a: Critical controls. This part is applicable to <u>all</u> Qualified Installations. Part 2b: PA-DSS Validated Applications. This part is applicable only to PA-DSS Validated Payment Applications.
Part 3: QIR Professional Additional Observations	Records observations or details that the Customer should be aware of. Includes items identified in the Details section that require explanation.

3.2.2 Ongoing Support

The QIR Professional may be asked to manage the Payment Application or other payment technologies after installation. This may include applying updates or patches, changing configurations, etc. The *QIR Implementation Statement* and the vendor documentation for the payment technologies should both be used during this work.

If a QIR Professional is troubleshooting or debugging for a Customer, any Cardholder Data that is collected must be encrypted while stored and securely deleted immediately after use.

If a QIR Professional is installing or supporting a point of sale technology, the QIR Professional or the Customer should not use that technology for unrelated functions (i.e. web browsing or email).

The QIR Professional must immediately report all known security vulnerabilities or identified security breaches, whether suspected or actual, to the Customer.

The QIR Professional must review, at least annually, updates to the applicable vendor documentation to remain current with all major and minor changes.

3.2.2.1   Remote Access

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

- Advise Customers to:
  - o   Turn on remote access only when necessary;
  - o   Monitor when in use; and
  - o   Turn off access immediately thereafter.
- Use remote access software only when absolutely necessary, and in a secure manner, to access Customer sites for installation, support, and maintenance purposes.
- Use multi-factor authentication with strong cryptography.

904717.1
962665.3

QIR Professionals using remote access software must follow the information provided by the application vendor in the vendor documentation, which may contain instructions on using remote access security features. The QIR Professional 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.

- Remote QIR Professional access to Customer sites must only come from specific IP addresses expected by the network design.

- Unique, complex, and secure authentication credentials must be used for each Customer.

- Data transmissions must always be encrypted.

3.2.2.2 PFI Support

If the QIR Professional is asked to participate in the investigation of a breach at the Customer environment where the QIR Professional installed any Payment Application, payment technologies, or otherwise performed Services or a Qualified Installation, the QIR Professional may be asked to provide copies of the *QIR Implementation Statement* and related documentation from the Engagement to the Customer and/or to the PCI Forensic Investigator (PFI), and must cooperate fully with the PFI in such investigation and all such requests.

3.2.3 Engagement Termination

When an Engagement ends, the QIR Professional must perform cleanup tasks that include, but are not limited to:

- Ensuring the QIR Professional's credentials not needed by the Customer are securely removed from all Customer sites after any installation or maintenance tasks have been completed

- Providing instructions for the Customer to remove QIR Professional user accounts and credentials, if the QIR Professional no longer supports the Customer

- Providing instructions for the Customer to eliminate all connectivity· for example, open firewall ports· between the QIR Professional and the Customer

3.3 Service Fees

Pricing and fees charged by QIR Professionals (or the companies that employ them) for the Services they provide to Customers in connection with Qualified Installations are negotiated directly between the QIR Professional (or the company that employs them) and the applicable Customer. PCI SSC is not involved in any way with any such fees or pricing.

4 QIR Quality Management

QIR Professionals must perform all aspects of their Qualified Installations and other Services in a high-quality, professional, competent, diligent, and well-informed manner.

Without limiting the foregoing, all Qualified Installations and Services must be performed in accordance with all applicable Qualification Requirements, including but not limited to, the requirements specified in the *QIR Program Guide*, the *QIR Qualification Requirements*, and the *QIR Implementation Instructions*. In order to help ensure the foregoing, PCI SSC engages in ongoing QIR Professional monitoring, through both direct interaction and *QIR Feedback Forms* received from Customers and third parties.

4.1 Quality Management – Role of QIR Professional

QIR Professionals are responsible for the quality of the Qualified Installations they lead or take part in, including all documentation provided to the Customer, and must adhere to all quality assurance requirements established by PCI SSC from time to time, including but not limited to the requirements specified in this *QIR Program Guide*, the *QIR Qualification Requirements,* and the *QIR Implementation Instructions*.

In order to help ensure the quality of each Qualified Installation, the QIR Professional should consider the following (as a minimum):

- Review the PCI DSS and related requirements that apply to the Qualified Installation. References are provided in the *QIR Implementation Instructions* available on the Website.

- Where available, review information documented in *QIR Implementation Statements* relating to similar installations.

- Thoroughly document all Qualified Installation results.

- Review all *QIR Implementation Statements* for quality and completeness before publication. The *QIR Implementation Instructions* contains a checklist of tasks to be completed as part of a Qualified Installation.

- Review all information provided in the vendor documentation on how to configure and support their products securely.

4.1.1 Feedback Process

At the start of each Qualified Installation, the QIR Professional must direct the Customer to the *QIR Feedback Form* on the Website and request that the Customer submit the completed form to PCI SSC following the installation.

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

The *QIR Feedback Form* addresses the following:

- Adequacy of *QIR Implementation Statement* content

- 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

4.2 Quality Management – Role of PCI SSC

The PCI SSC quality assurance process begins with the QIR Professional Qualification and related training process.

PCI SSC then performs monitoring activities to gain assurance that established requirements are in place and maintained as expected. This is achieved most often through review and monitoring of *QIR Feedback Forms* and may include audits of *QIR Implementation Statements* and other materials, information, or work product generated or obtained during the course of Qualified Installations. PCI SSC reserves the right to conduct such activities at any time, and each QIR Professional is required to cooperate in such quality assurance activities.

Note: The QIR Professional may redact sensitive or confidential information that does not materially impact PCI SSC's quality assurance review.

Failure to satisfy applicable requirements or meet applicable quality levels may result in any or all of the actions described in Section 5.3 below.

5   QIR Professional Status

The QIR Program recognizes several status designations for QIR Professionals. The status of a QIR Professional is initially Good Standing but this may change based on quality concerns, feedback, administrative issues, or other factors. These status designations are described below.

Status designations are not necessarily progressive: Any QIR Professional's status may be revoked for quality concerns or failure to satiafy applicable Qualification Requirements. Accordingly, a QIR Professional may move directly from Good Standing to Revocation. Non-severe quality concerns are generally addressed through the Remediation process (described below) in order to promote improved performance.

5.1   Good Standing

QIR Professionals are expected to maintain a status of Good Standing while participating in the QIR Program. Where PCI SSC detects any deterioration of quality levels over time, PCI SSC may issue warnings to QIR Professionals. While a Warning should be taken seriously so that actions do not escalate to Remediation and/or Revocation, a Warning alone does not impair a QIR Professional's Good Standing status.

5.2   Remediation

Participation in the QIR Program remediation process ("Remediation") may be required for various reasons, including quality concerns or administrative issues· such as failure to meet any requalification requirements, failure to submit required information, etc. QIR Professionals in Remediation are listed on the Website in **red**, indicating Remediation status without further explanation as to why the designation is warranted.

If administrative or non-severe quality problems are detected, PCI SSC will typically recommend participation in the Remediation program, which provides an opportunity for QIR Professionals to improve performance by working closely with PCI SSC staff.

During Remediation, QIR Professionals may continue to perform Qualified Installations and other Services. During Remediation and generally in connection with PCI SSC's QIR Program quality assurance initiatives, PCI SSC may monitor and require QIR Professionals to provide *QIR Implementation Statements* and any other materials, information, or work product generated or obtained during the course of Qualified Installations (redacted in accordance with QIR Program policy). Such materials must be provided within three (3) weeks of PCI SSC's request. QIR Professionals may also be charged fees to cover PCI SSC's costs of monitoring and Remediation.

Remediation is a joint effort between the QIR Professional and PCI SSC to improve the quality of the QIR Professional's work. To participate in Remediation, the QIR Professional must agree to comply with all Remediation requirements and conditions specified by PCI SSC, including but not limited to, submission of a Remediation plan acceptable to PCI SSC, which details how the QIR Professional plans to improve the quality of its Qualified Installations and related work product.

5.3   Revocation

In the event PCI SSC determines in its sole but reasonable discretion that a QIR Professional meets any condition for revocation of QIR Professional Qualification established by PCI SSC from time to time (satisfaction of any such condition, a "Violation"), including without limitation, any of the conditions described as Violations below, PCI SSC may, effective immediately upon notice to the

QIR Professional, revoke the QIR Professional Qualification ("Revocation"). Violations include (without limitation):

- Violation of any obligation regarding non-disclosure of confidential materials

- Failure to maintain physical, electronic, and procedural safeguards to protect confidential or sensitive information; and/or failure to report to PCI SSC unauthorized access to any system that stores confidential or sensitive information

- Engagement in unprofessional or unethical business conduct, including misrepresentation of the PCI DSS or any other PCI SSC requirements or documents in order to sell products or services

- Failure to provide quality services, based on Customer feedback or evaluation by PCI SSC, any of its affiliates, or any third party

- Cheating on any exam in connection with QIR Program training, including without limitation submitting work that is not the work of the QIR Professional 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

- Provision of false or intentionally incomplete or misleading information to PCI SSC in any application or other materials

- Permitting any person or entity other than a QIR Professional to perform (or participate in the performance of) any Qualified Installation for or on behalf of the QIR Professional

- Failure to be in Good Standing

- Failure to perform any Qualified Installation in accordance with the *QIR Program Guide* or applicable Qualification Requirements

- Revelation by forensic evidence that any act or omission of, or condition created by the QIR Professional (whether as part of its Services or otherwise) was a material factor in causing a security or data breach of any of their QIR Customers

- Failure to promptly notify PCI SSC of any Violations described above that occurred less than two (2) years before such QIR Professional's qualification by PCI SSC

Upon QIR Professional Revocation, the QIR Professional is removed from the QIR List and/or its listing may be annotated as PCI SSC deems appropriate, and the QIR Professional must (a) immediately cease all advertising and promotion of its QIR Professional Qualification and/or status; (b) immediately cease soliciting for and performing all pending Engagements, Qualified Installations, or other Services unless and to the extent otherwise instructed by PCI SSC; (c) if requested by PCI SSC, obtain (at the QIR Professional's sole cost and expense) the services of a replacement QIR Professional acceptable to PCI SSC for purposes of completing any unperformed Services for which it is engaged immediately prior to such Revocation or termination; and (d) within fifteen (15) days thereof, in a manner acceptable to PCI SSC, notify those of its Customers with which the QIR Professional is then engaged to perform Services of such Revocation or termination and, if applicable, of any conditions, restrictions, or requirements of such Revocation that may impact its ability to perform such Services for Customers going forward. PCI SSC may notify any third party of such Revocation or termination and the reason(s) therefor.

Revocation is subject to appeal and possible reinstatement of qualification in accordance with QIR Program policies and procedures. All appeals must be submitted to PCI SSC in writing within thirty (30) days of Revocation, addressed to the PCI SSC QIR Program Manager, and must follow all applicable procedures as specified by PCI SSC. All determinations of PCI SSC regarding Revocation and any related appeals are in PCI SSC's sole discretion, final, and binding upon the QIR Professional. In the event the QIR Professional fails to submit a request for appeal within the allotted 30-day period, or if PCI SSC determines on appeal that termination is warranted, then effective immediately and automatically thereafter, the QIR Professional Qualification shall terminate.

Upon Revocation, the period of ineligibility will be a minimum of one (1) year (to be 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.

Appendix A: Acceptable Forms of Documented Evidence

For a minimum of three (3) years after conducting a Qualified Installation, QIR Professionals 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 QIR Professional must maintain adequate physical, electronic, and procedural safeguards consistent with industry-accepted practices to protect sensitive and confidential information against loss or unauthorized access during storage, processing, and/or transmitting of this information.

All such documented evidence must be made available to PCI SSC, PFIs, and Participating Payment Brands upon request, for the time period specified above, even if the QIR Professional has left the QIR Program.

These are the acceptable forms of documented evidence:

- Copies of any logs or configuration files used or generated

- Copies of any Payment Application or payment technology vendor written/published documentation used

- Copies of any troubleshooting requests raised with the Payment Application or payment application or technology vendor during or as a result of the implementation

- Any written/published Payment Application or payment technology 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 displays of payment card data when displayed on, 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