Payment Card Industry (PCI)

Qualified Integrator and Reseller (QIR)™

Implementation Instructions

Version 4.0

March 2018

Document Changes

Date	Version	Description
August 2012	1.0	Original Publication
November 2014	2.0	Update to align with PCI DSS and PA-DSS v3.0
August 2015	2.1	Update to align with PCI DSS and PA-DSS v3.1
September 2015	3.0	Update to align with QIR Program Guide & Qualification Requirements, v3.0
March 2018	4.0	Update to reflect QIR Program Expansion

Contents

Introduction

When performing a Qualified Installation, the QIR Professional is required to complete a *QIR Implementation Statement,* and the instructions on how to do so are provided in this document.

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

Notes:

1. *If an application being installed or configured is PA-DSS validated, Part 2b of the statement should be completed.*
2. *The customer may request the QIR Professional to complete work beyond the scope of the QIR Program. This work should not be documented as part of the Qualified Installation.*
3. *By signing the QIR Implementation Statement, the QIR Professional indicates and affirms that all instructions within the QIR Program Guide and these QIR Implementation Instructions have been followed.*
4. *This document is written as if Engagements and Qualified Installations are carried out by one QIR Professional. In the event that a larger project involves more than one QIR Professional, one of those individuals should be nominated as the primary or lead.*

QIR Professionals must adhere to the requirements defined in the *QIR Qualification Requirements* and *QIR Program Guide* for all Qualified Installations. Additionally, the *QIR Program Guide* details the activities that QIR Professionals are required to perform during Qualified Installations. Examples of these include:

- Where any new applications being installed claim PA-DSS Validation status, confirming that they appear on the list of *Validated Payment Applications* on the PCI SSC website
- Protecting confidential and sensitive information at all times
- Providing the customer with a completed *QIR Implementation Statement* for each Qualified Installation
- Encouraging the customer to complete and return the *QIR Feedback Form* to PCI SSC
- Maintaining records of the Qualified Installation

A copy of the *QIR Implementation Statement* must be delivered to the customer no later than ten (10) business days after completion of the Qualified Installation, and a copy must be retained by the QIR Professional with their work papers.

Completing the QIR Implementation Statement

The *QIR Implementation Statement* has three (3) parts:

Part 1: Implementation Statement Summary	Records details about the customer, the QIR Professional and the services provided under the Qualified Installation, whether onsite or remotely. Includes required signatures for the customer acknowledgement 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 all Qualified Installations. ▪ Part 2b: PA-DSS Validated Payment Applications. This part is applicable only to PA-DSS Validated Payment Application installations.
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.

The *QIR Implementation Statement* is designed to be completed by the QIR Professional, either electronically and then printed for signature by the QIR Professional and Customer Company contact, or printed out as a hard-copy document for manual completion and signature by both parties. For all Yes/No questions, if ***Yes*** is selected, all bulleted questions below the entry must also be answered.

Part 1: Implementation Statement Summary

Part 1, the Implementation Statement Summary, requires information about the customer and QIR Professional engaged in the Qualified Installation, the customer's environment, the payment application being installed and/or configured and the agreed results of the Qualified Installation:

Item for Completion	Instruction
Customer Details	
Customer company and contact details:	Provide customer company and individual contact name. Complete contact and address details as stated.
QIR Details	
QIR Professional with their company and contact details:	Provide QIR Professional contact name. Complete contact and address details as stated.
Details of Payment Application	
Payment Application Vendor:	Provide the name of the payment vendor company that produced the application.
Payment Application Name:	Provide the name of the payment application.
Application Version Number:	Provide the specific version number for the payment application.
Details of Qualified Installation	
Address of impacted customer location(s):	List of all addresses where the QIR Professional performed the services of the Qualified Installation as represented by the *QIR Implementation Statement*. For example, there may be multiple retail locations, corporate offices, or other types of locations where the application was installed as part of the Qualified Installation. The location of every installation covered by the *QIR Implementation Statement* must be included in this table. 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. If there are a number of QIR Professionals leading separate Qualified Installations on a larger project, each QIR Professional must produce their own *QIR Implementation Statement(s)* for the installations they were responsible for. Limit of one customer address per row. Note that the QIR Professional may insert additional rows to this table if needed. Where the Qualified Installation was performed remotely, the QIR Professional may indicate this here.
Services performed under Qualified Installation:	Provide a brief description of the services performed under the Qualified Installation. For example, payment applications installed or upgraded, their platforms, and any other relevant systems or hardware installed or changed.

Item for Completion	Instruction
QIR Acknowledgement of Implementation Statement	
The QIR Professional is required to sign the *QIR Implementation Statement* affirming the findings documented therein. By signing the *QIR Implementation Statement*, the QIR Professional acknowledges the following: • The installation was performed in accordance with the requirements defined in the *QIR Qualification Requirements*, *QIR Program Guide* and these *QIR Implementation Instructions*. • All information within the *QIR Implementation Statement* represents the results of the implementation fairly and accurately in all material respects. • The QIR Professional has advised the customer of any potential security risks observed, or other relevant observations identified during the Qualified Installation, as documented in Part 3 of the *QIR Implementation Statement*.	
QIR Professional Signature:	Signature of the QIR Professional for the Qualified Installation
QIR Professional Name:	First and last name of the QIR Professional
Date:	Date the *QIR Implementation Statement* was signed
Customer Acknowledgement of Implementation Statement	
The customer signs the *QIR Implementation Statement* to acknowledge the following: • The *QIR Implementation Statement* is an accurate record of the work completed by the QIR Professional. • The customer has read and understands the potential security risks identified in Part 3 of the *QIR Implementation Statement*. • The customer understands they are responsible for maintaining their PCI DSS compliance and that any changes to their systems or environment should be made in accordance with PCI DSS Requirements.	
Customer Contact Signature:	Signature of the customer contact accepting the *QIR Implementation Statement*
Customer Contact Name:	First and last name of the customer contact
Date:	Date the *QIR Implementation Statement* was signed

Part 2: Implementation Statement Details

Part 2 of the *QIR Implementation Statement* requires the QIR Professional to provide details regarding the Qualified Installation and verify that the QIR Professional has addressed the critical controls affecting the security of cardholder data. All questions in Part 2 require an answer. All answers of ***No – Details provided in Part 3*** require an explanation in Part 3 of the *QIR Implementation Statement*. All answers of ***Yes*** indicate that the QIR Professional has done at least one of the following:

- Provided the customer with the item(s) indicated in the question—typically a list, a form, etc. Any such items should be provided in writing so that the QIR Professional and the customer can retain copies.
- Discussed with the customer or otherwise gained confidence that the customer is aware and has an understanding of a requirement, technical knowledge, or a process that must be in place. QIR Professional confidence can be achieved in a variety of ways including:
    - Reviewing customer documentation
    - Interviewing appropriate customer employees
    - Conducting training/education sessions
- Confirmed through the installation/configuration process that the application and configuration is as expected. Evidence should be captured with a screenshot or documentation as part of the QIR Professional's work papers.

Part 2 is divided into two sections:

- Part 2a: Critical Controls. This part is applicable to all Qualified Installations.
- Part 2b: PA-DSS Validated Payment Applications. This part is applicable only to PA-DSS Validated Payment Application installations.

Part 2a: Critical Controls

This part is applicable to all Qualified Installations.

Item for completion	Instruction	PCI DSS Reference
Remote Access		
1. Is the customer aware that any remote access into their network must be configured as follows:		
• Remote access to the payment application requires multi-factor authentication?	Select “Yes” or “No” from the drop-down menu. A response of “Yes” indicates that the QIR Professional has confidence that the customer understands that multi-factor authentication is required for any remote access to the payment application or to the customer’s cardholder data environment. Multi-factor authentication requires that a minimum of two of the three following authentication methods be used for authentication in addition to a unique user ID: • A password or passphrase (Something you **know**) • A token device or smart card (Something you **have**) • A biometric (Something you **are**) Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.	PCI DSS Requirement 8.3
• Remote access must be activated only when needed, monitored when in use, and immediately deactivated after use?	Select “Yes” or “No” from the drop-down menu. A response of “Yes” indicates that the QIR Professional has confidence that the customer understands that any third party remote access to their network must be activated only when needed and monitored when in use. The customer is further aware that remote access must be deactivated immediately when no longer needed.	PCI DSS Requirements 8.1.5 and 12.3

Item for completion	Instruction	PCI DSS Reference
• Remote access must be implemented securely?	Select "Yes" or "No" from the drop-down menu. A response of "Yes" indicates that the QIR Professional has confidence that the customer understands that any remote access to their network must be implemented in a secure manner, such as: • Default settings in the remote access software are changed—for example, change default passwords and use unique passwords for each customer. • Connections are allowed only from specific (known) IP/MAC addresses. • Strong authentication and complex passwords for logins are used. • Encrypted data transmission is enabled. • Account lockout after a certain number of failed login attempts is enabled. • Virtual Private Network ("VPN") connections are established via a firewall before access is allowed. • The logging function is enabled. • Access to accounts on the customer network is restricted to authorized integrator/reseller personnel. • Customer passwords are established according to PCI DSS Requirements. Additionally, any systems used for remote access into the customer environment should meet applicable PCI DSS requirements. For example, desktops/laptops must have up-to-date patches, anti-virus and be protected by a firewall.	PCI DSS Requirements 1.4, 5 ,6.2, 8
2. Will any QIR personnel access the customer site remotely or configure remote access on behalf of the customer? *Check either the "Yes" or "No" box. If the "Yes" box is checked, the applicable bullet points must also be answered:*		
Yes. The QIR personnel are using and/or configuring remote access to the customer site:	Checking the "Yes" box for this question indicates that QIR personnel will be accessing the customer site remotely or will be configuring remote access on behalf of the customer.	
• Is remote access implemented to require multi-factor authentication?	Select "Yes" or "No" from the drop-down menu. A response of "Yes" indicates that all QIR personnel are required to use multi-factor authentication when accessing the customer site remotely.	PCI DSS Requirement 8.3

Item for completion	Instruction	PCI DSS Reference
• Does the customer have a process to ensure that remote access to the customer network is activated only when needed, access is monitored when in use, and is immediately deactivated after use?	Select “Yes” or “No” from the drop-down menu. A response of “Yes” indicates that the customer has a process in place to activate remote access only when QIR personnel need it, to monitor access while in use and to deactivate remote access immediately when it is no longer needed.	PCI DSS Requirement 12.3.9
• Is remote access to the customer network implemented securely?	Select “Yes” or “No” from the drop-down menu. A response of “Yes” indicates that QIR personnel remotely access the customer network in a secure manner. QIR personnel implement security features for remote access, such as: • Default settings in the remote access software are changed—for example, change default passwords and use unique passwords for each customer. • Connections are allowed only from specific (known) IP/MAC addresses. • Strong authentication and complex passwords for logins are used. • Encrypted data transmission is enabled. • Account lockout after a certain number of failed login attempts is enabled. • Virtual Private Network (“VPN”) connections are established via a firewall before access is allowed. • The logging function is enabled. • Access to accounts on the customer network is restricted to authorized integrator/reseller personnel. • Customer passwords are established according to PCI DSS Requirements. Additionally, QIR personnel should only connect to their customers from systems that meet applicable PCI DSS Requirements. For example, QIR personnel desktops/laptops must have up-to-date patches, anti-virus and be protected by a firewall.	PCI DSS Requirements 1.4, 5, 6.2. 8.
No. The QIR will not access the customer site remotely and will not configure remote access on behalf of the customer.	Checking the “No” box for this question indicates that the QIR Professional is physically on site at the customer’s place of business and will not be accessing the customer’s site remotely for any purpose. Additionally, the QIR Professional will not be configuring the customer’s remote access.	

Item for completion	Instruction	PCI DSS Reference
Accounts and Passwords		
3. Have all passwords been changed for all payment application default accounts (including all user and administrative accounts)?	Select "Yes" or "No" from the drop-down menu. A response of "Yes" indicates that all passwords have been changed for: • All payment application user default accounts, and • All payment application administrative default accounts. Default accounts are accounts or user IDs that are created by the payment application vendor and included in the application when it is delivered to the customer. Some are created for the general user of the application and may not have many privileges or rights; while other default accounts are administrative accounts and may be delivered with all privileges and rights enabled. These default accounts will not be unique per customer so the passwords must be changed, at a minimum. **All default account passwords must be changed, irrespective of the type of account or the level of privilege assigned.** If dependent or underlying software—such as databases or operating systems—are provided as part of the Qualified Installation, passwords for those default accounts must also be changed. Default accounts that are not needed should be changed (even if they won't be used) and then disabled or deactivated.	PCI DSS Requirement 2.1

Item for completion	Instruction	PCI DSS Reference
4. Is strong authentication and multi-factor authentication configured for all payment application administrative accounts and strong authentication configured for all application accounts with access to cardholder data?	Select "Yes" or "No" from the drop-down menu. A response of "Yes" indicates that the QIR Professional has confirmed that strong authentication is configured for: • All application accounts with administrative access, and • All application accounts with access to cardholder data Also that multi-factor authentication is configured for: • All application accounts with administrative access This includes all credentials that are generated or managed by the payment application. Strong authentication is created in accordance with PCI DSS Requirements 8.5.8 through 8.5.15, and includes: • Not using group, shared, or generic accounts and passwords, or other authentication methods • Changing user passwords at least every 90 days • Requiring a minimum password length of at least seven characters • Using passwords containing both numeric and alphabetic characters • Not allowing an individual to submit a new password that is the same as any of the last four passwords he or she has used • Locking out the user ID after not more than six attempts • Setting the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID • Requiring users to re-authenticate after 15 minutes of an idle session Strong credentials need to be in place by the completion of the application's installation and for subsequent changes after installation. If dependent or underlying software—such as databases or operating systems—are provided as part of the Qualified Installation, strong authentication must also be configured for these accounts.	PCI DSS Requirements 8.1.6 - 8.1.8, 8.2.3 - 8.2.5, 8.3, 8.5

Item for completion	Instruction	PCI DSS Reference
5. Is the customer aware that all access to systems containing cardholder data (such as PCs, servers, and databases) should use unique user IDs and strong authentication?	Select "Yes" or "No" from the drop-down menu. A response of "Yes" indicates that the QIR Professional has confidence that the customer understands that all access to any system containing cardholder data should use unique accounts and strong authentication. This includes, for example, user and administrative accounts on PCs, servers, databases, and other system components within the CDE. Strong authentication should be implemented in accordance with the instructions provided in Question 4 above (per PCI DSS Requirements 8.5.8 – 8.5.15).	PCI DSS Requirements 8.1 and 8.2
6. Is the customer aware that, for all accounts used by operating systems (such as security software, applications, systems, POS terminals): a. All vendor-supplied defaults should be changed, and b. All unnecessary default accounts should be removed or disabled?	Select "Yes" or "No" from the drop-down menu. A response of "Yes" indicates that the QIR Professional has confidence that the customer understands that all vendor-supplied defaults should be changed for all accounts used by operating systems, security software, applications and systems, POS terminals, etc., and that all unnecessary default accounts should be removed or disabled.	PCI DSS Requirement 2.1
7. Are all QIR personnel using unique accounts and passwords for each customer location?	Select "Yes" or "No" from the drop-down menu. A response of "Yes" indicates that the QIR Professional has ensured that all personnel with access to any customer location have a unique user account and a unique password for each customer location. Default or shared accounts must not be used. QIR personnel must not use the same account or password for multiple customers.	PCI DSS Requirement 8
8. Is the customer aware of all accounts set up by or used for QIR personnel access, and have instructions been provided on how to change the passwords and disable or remove those accounts?	Select "Yes" or "No" from the drop-down menu. A response of "Yes" indicates that the QIR Professional has provided the customer with: • A list of all accounts that were created by the QIR Professional, including those for the customer's use • A list of all accounts used by QIR personnel • Instructions on how to change passwords for, and disable or remove, all accounts used by QIR personnel This includes all accounts created for the payment application, any dependent software accounts, any operating system accounts, network access accounts, etc. The QIR Professional has confidence that the customer understands how to change the passwords for all accounts created. The customer also understands how to disable or remove those accounts.	PCI DSS Requirement 2.1

Item for completion	Instruction	PCI DSS Reference
Patching		
9. Have the latest vendor-supplied security patches and updates been applied to all software installed by the QIR Professional, including the payment application?	Select "Yes" or "No" from the drop-down menu. A response of "Yes" indicates that the QIR Professional has confirmed that the latest security patches and updates provided by the vendor have been applied. This includes the payment application and any software installed by the QIR Professional, such as dependent or underlying software or operating systems. If dependent or underlying software—such as databases or operating systems—are provided as part of the Qualified Installation, the QIR Professional should configure the operating system and underlying software in accordance with all applicable PCI DSS Requirements.	PCI DSS Requirement 6.1
10. Is the customer aware that vendor-supplied security patches and updates must be applied to the payment application and any underlying software or systems?	A response of "Yes" indicates that the QIR Professional has confidence that the customer understands the need to apply vendor security patches and updates for the payment application and any dependent software or operating systems in their payment environment. They further understand that they should install critical security patches within one month of release.	PCI DSS Requirement 6.2

Part 2b: PA-DSS Validated Payment Applications

This part is applicable only to PA-DSS Validated Payment Application installations.

Item for completion	Instruction
If a PA-DSS Validated Application was installed, the following information should be provided:	
PCI SSC Listing Number:	Provide the PCI SSC listing number for the specific version of the validated payment application, as listed on the PCI SSC website.
Payment Application Vendor:	Provide the name of the payment vendor company that produced the application. This name should match the company name listed on the PCI SSC website for this payment application.
Payment Application Name:	Provide the name of the validated payment application. This name should match the application name listed on the PCI SSC website.
Application Version Number:	Provide the specific version number for the validated payment application. This version number must match the application listing on the PCI SSC website, and the application should be approved for new deployments, in order for the application to be considered PA-DSS validated.
The validated payment application was installed in accordance with the ***PA-DSS Implementation Guide*** *(Yes/No)* *If "No", please provide a brief explanation:*	Select "Yes" or "No" from the drop-down menu. "Yes" indicates that all applicable instructions in the *PA-DSS Implementation Guide* were followed, and that the QIR Professional installed the application according to *PA-DSS Implementation Guide* instructions. Note that using these Q*IR Implementation Instructions* with the *PA-DSS Implementation Guide* during a Qualified Installation provides the foundation for a payment application installation that is configured in a manner that supports compliance with PCI DSS. If the customer does not have access to the *PA-DSS Implementation Guide,* one can be requested from the payment application vendor. "No" indicates that QIR Professional did not follow the *PA-DSS Implementation Guide.* If "No" is selected, the QIR Professional should provide an explanation in the text field provided regarding why they could not use the *PA-DSS Implementation Guide* for the Qualified Installation. For example, the QIR Professional may be unable to use the *PA-DSS Implementation Guide* if it did not contain the level of instruction necessary to configure the application securely, or if following the *PA-DSS Implementation Guide* in the customer's environment would result in an insecure or non-compliant configuration.
Date and version of the *PA-DSS Implementation Guide* used during the installation of the payment application:	Record the version number and the date of the *PA-DSS Implementation Guide* that was used during the Qualified Installation.

Part 3: QIR Professional Additional Observations

Part 3, QIR Professional Additional Observations, has several purposes. The first is to provide details of all responses where the QIR Professional selected *"No – Details provided in Part 3."* Each "No" response must be explained in its own row. Secondly, the QIR Professional should include any observations or details they feel the customer should be aware of, including any potential security risks the QIR Professional is aware of in the customer environment.

Observations included in this section in no way imply that a PCI DSS assessment has been completed.

Where aspects of the installation were performed by parties other than the QIR Professional (for example, the customer or other third party), the QIR Professional should provide relevant details in this section.

The table should be completed as follows:

Column	Guidance
Observation #:	Sequential number from 1 to N, to identify each observation.
Observation Details:	Record any observations that the QIR Professional wishes to bring to a customer's attention, including any potential security risks and any items from Part 2 with a response of *"No – Details provided in Part 3."*
Applicable Subject and Question Number from Part 2:	If the observation relates to a question from Part 2 of the *QIR Implementation Statement*, record the applicable question number here.
Potential security risks?	If the QIR Professional feels that the observation could possibly affect or have an impact on the customer's security risks, check "Yes." If the observation is not relevant to any security risk, check "No." ***Note:*** *It is not the QIR Professional's responsibility to determine PCI DSS compliance for their customer. Potential compliance issues may or may not be an indication of an actual compliance issue; however, this is for the customer to determine.*
PCI DSS reference (if applicable):	If the observation has potential relevance to a PCI DSS Requirement, identify the specific PCI DSS Requirement here.

Observation Examples

Examples of observations are provided below.

***Note**: These are examples only and are provided to assist the QIR Professional understand how the table is to be used to record their observations.*

Observation #	Observation Details	Applicable subject and question number from Part 2	Potential security risks?		PCI DSS reference (if applicable)
			Yes	No	
1	The customer has delayed installation of a recent vendor-supplied security patch for the payment application.	Patching – Question 9, 10	☒	☐	PCI DSS Requirements 6.1 and 6.2
2	There does not appear to be a process in place to ensure that remote access to the customer's network is activated only when needed.	Remote Access – Question 2	☒	☐	PCI DSS Requirements 8.1.5 and 12.3.9
3	The underlying operating system has insecure services running and the anti-virus software is out of date.	N/A	☒	☐	PCI DSS Requirements 2 and 5
4	The underlying system contains old stores of cardholder data that are not encrypted.	N/A	☒	☐	PCI DSS Requirements 3.1 and 3.4

***Note**: The QIR Professional may adjust column width and add/remove rows as needed to record all their observations. However, the QIR Professional must not remove any columns or change column headings.*