Payment Card Industry (PCI)

# Qualified Integrators and Resellers™

## Implementation Instructions

**Version 2.0**

November 2014

# 1 Introduction

When performing a Qualified Installation, the QIR Employee is required to complete the *QIR Implementation Statement* to record the details of the installation and configuration of the payment application. Details for how to complete the *QIR Implementation Statement* are provided in this document.

> ***Note:*** *By signing the* QIR Implementation Statement *the QIR Employee indicates and affirms that all instructions within the* QIR Program Guide *and these* QIR Implementation Instructions *have been completed.*

Use of these *QIR Implementation Instructions* with the *PA-DSS Implementation Guide* during a Qualified Installation provides the foundation for ensuring that the payment application will be installed and 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.

QIR Employees must adhere to the *QIR Qualification Requirements* at all times. Additionally, the *QIR Program Guide* details the activities that QIR Employees are required to perform, including those to be performed during Qualified Installations. Examples of these include:

- Ensuring personnel performing Qualified Installations are properly trained and screened as appropriate
- Confirming that any new applications being installed appear on the PCI SSC 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
- Maintaining a quality assurance program

QIR Employees are expected to follow the *QIR Program Guide* for all Qualified Installations.

# 2 Completing the QIR Implementation Statement

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

| | |
|---|---|
| Implementation Statement Summary | Records details about the customer, the QIR Company and QIR Employees and the payment application. Includes required signatures for the customer acceptance and the QIR Employee affirmation of the Qualified Installation. |
| Implementation Statement Details | Records details about the activities performed by the QIR Employee during the Qualified Installation. |
| QIR Employee 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 Employee either electronically and then printed for signature capture, or printed out as a hard copy document for manual completion and signature capture.

The *QIR Implementation Statement* consists of three types of fields:

***Free Standing Text*** – Free Standing Text fields appear as gray rectangles (       ). They do not have a maximum character limit and are intended to be filled by clicking on the field then proceeding to enter text. The gray rectangle will disappear when text is being entered.

***Drop Down Selections*** – Drop Down Selections (Choose an item.) will display a drop down arrow when the field is clicked on. Clicking on the drop down arrow will provide a range of acceptable responses. Selecting a response will populate the field with that response.

***Yes/No Checkboxes*** – Yes/No Checkboxes ( □ ) are gray boxes outlined with a black square. For these types of questions, the answer will be **Yes** or **No**. If **Yes** is selected, all bulleted questions must be responded to.

**Implementation Statement Details:**

Guidance for understanding the instructions provided in the Implementation Statement Details is provided below.

- Example instruction: "A response of "Yes" indicates that the QIR Employee has provided the customer with…"
  - ❖ The QIR Employee is to provide the customer with the item indicated in the instruction, typically a list, a form, etc.
  - ❖ This item should be provided  in writing so that copies can be retained by the QIR Company and the customer
- Example instruction: "A response of "Yes" indicates that the QIR Employee has confidence that the customer understands…"
  - ❖ The QIR Employee is being asked to make sure that the customer is aware of and has an understanding of a requirement, technical knowledge or a process that must be in place.
  - ❖ Gaining confidence that a customer "is aware of" or "has an understanding of" can be achieved in a variety of ways including:
    - ▪ Reviewing customer documentation
    - ▪ Interviewing appropriate customer employees
    - ▪ Conducting training/education sessions
- Example instruction: "A response of "Yes" indicates that the QIR Employee has confirmed that…" or "A response of "Yes" indicates that the QIR Employee has ensured that…"
  - ❖ The QIR Employee is being asked to make sure that an activity has taken place, for example, configuring software, enabling a parameter, application of patches.

- Evidence of these types of activities can be captured with a screenshot or documentation as part of the QIR Employee’s work papers.

## *Part 1: Implementation Statement Summary*

Part 1, the Implementation Statement Summary, requires information about the customer and QIR Company and QIR Employee 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 in QIR Implementation Statement*** | ***Instruction for QIR Employee to complete*** |
|---|---|
| ***Customer Details*** | |
| Customer Company and Contact Details: | Provide customer company and individual contact name.<br>Complete contact and address details as stated. |
| ***QIR Details*** | |
| QIR Company and Contact Details: | Provide QIR Company and Employee contact names.<br>Complete contact and address details as stated. |
| ***PA-DSS Validated Payment Application*** | |
| PCI SSC Listing Number: | Provide the PCI SSC listing # 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 who 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 in order for the application to be considered PA-DSS validated. |
| ***Details of Qualified Installation*** | |
| Address of customer location(s) where application was installed: | List of all addresses where the QIR Employee installed the payment application as represented by the 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.<br>The location of every installation covered by the Implementation Statement must be included in this table.  Where a Qualified Installation involves multiple customer locations, the QIR Employee may choose to prepare a number of Implementation Statements that together represent all locations.<br>If there are a number of QIR Employees leading Qualified Installations, each Lead QIR Employee must produce his or her own Implementation Statement(s) for the installations he or she were responsible for.<br>Limit to one customer address per row. Note that the QIR Employee may insert additional rows to this table if |

| | |
|---|---|
| | needed. |
| Type of systems application installed on: | Provide a brief description on the type of systems on which the application was installed.  For example, mainframe, POS, server, etc. |
| Number of systems installed: | Provide the number of systems the application was installed on at each location.  For example, a single retail location may have 20 POS systems and one server. |
| Type of Qualified Installation: | Select from the drop-down menu whether the installation is a New Installation or an Upgrade to an Existing Installation.  A New Installation is one where the payment application did not previously exist.  An Upgrade to an Existing Application can be an update applied to an application already installed, or a new version of an application already installed. |
| Date Installed: | For each address listed, provide the date(s) the application was installed.  If the installation occurred over a number of days, the date may be represented as a range – for example, 10-14 June 2012. |
| ***Confirmation of Implementation Approach*** | |
| This Implementation Statement confirms that: | |
| The validated payment application was installed in accordance with the ***PA-DSS Implementation Guide*** *(Yes/No)*<br>*If "No", please provide a brief explanation:* | Select "Yes" or "No" from the drop-down menu.<br>"Yes" indicates that all applicable instructions in the PA-DSS Implementation Guide were followed, and that the QIR Employee did not install the application contrary to Implementation Guide instructions.<br>"No" indicates that QIR Employee did not follow the PA-DSS Implementation Guide for one or more PCI DSS requirements.<br>If "No" is selected, the QIR Employee should provide an explanation in the text field provided, of why they could not use the PA-DSS Implementation Guide  for the Qualified Installation.<br>For example, the QIR Employee 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 that following the Implementation Guide would result in an insecure or non-compliant configuration. |
| The validated payment application was installed and in a manner that supports **compliance with PCI DSS** *(Yes/No)*<br>*If "No", reasons must be documented in Part 3.* | Select "Yes" or "No" from the drop-down menu.<br>An answer of "Yes" indicates that, to the best of the QIR Employee's knowledge, the payment application and its configuration settings have been installed in a PCI DSS compliant manner.<br>An answer of "No" indicates that the QIR Employee is aware that the application has been configured in a manner that is not compliant with or does not support PCI DSS requirements.  If the customer requested the application be configured in a way that does not meet PCI DSS requirements, the QIR Employee must advise the customer of such, and provide details in Part 3 of the Implementation Statement.<br>If aspects of the installation were performed by parties other than the QIR Employee (for example, by the customer), the QIR Employee should provide details in Part 3 of the Implementation Statement. |

***QIR Acceptance of Implementation Statement***

The Lead QIR Employee is required to sign the Implementation Statement affirming the findings documented therein. By signing the QIR Implementation Statement, the Lead QIR Employee acknowledges the following:

- The installation was performed in accordance with the requirements defined in the QIR Qualification Requirements, QIR Program Guide and QIR Implementation Instructions.
- All information within the Implementation Statement represents the results of the implementation fairly and accurately in all material respects.
- The Lead QIR Employee has advised the customer of any potential PCI DSS compliance issues identified during the implementation, as documented in Part 3 of the Implementation Statement.

| | |
|---|---|
| *Lead QIR Employee Signature:* | Signature of the Lead QIR Employee for the Qualified Installation |
| *Lead QIR Employee Name:* | First and last name of the Lead QIR Employee |
| *Date:* | Date the Implementation Statement was signed |
| *QIR Peer Review Employee Signature:* | Signature of the QIR Employee performing Peer Review of the Implementation Statement |
| *QIR Peer Review Employee Name:* | First and last name of the QIR Employee performing the Peer Review |
| *Date:* | Date the Implementation Statement was signed |

***Customer Acceptance of Implementation Statement***

The customer is required to sign the Implementation Statement confirming that they agree with and accept the findings documented therein. By signing the Implementation Statement, the customer acknowledges the following:

- The customer accepts the information documented within this Implementation Statement.
- The customer has read and understands all potential compliance issues identified in Part 3 of the Implementation Statement.
- The customer understands they are responsible for maintaining their PCI DSS compliance and that that any changes to the payment application or underlying systems should be made in accordance with PCI DSS Requirements.

| | |
|---|---|
| *Customer Contact Signature:* | Signature of the customer accepting the Implementation Statement |
| *Customer Contact Name:* | First and last name of the customer |
| *Date:* | Date the Implementation Statement was signed |

## Part 2: Implementation Statement Details

Part 2 of the Implementation Statement requires the QIR Employee to provide details regarding the Qualified Installation, and verify that the QIR Employee has addressed the most common threats and vulnerabilities that may impact 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 Implementation Statement.

| ***Item for completion in QIR Implementation Statement*** | ***Instruction for QIR Employee to complete*** |
|---|---|
| **PA-DSS Implementation Guide and Training Materials Used** | |
| 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. |
| Details of payment application training materials reviewed prior to the installation (including document name, version, date): | Briefly describe the training materials reviewed. For example, training materials provided by the vendor, webinars, classes, reference guides, etc. Include the name of the training material reviewed, the version (if applicable) and the date of the material. |

| ***Item for completion in QIR Implementation Statement*** | ***Instruction for QIR Employee to complete*** | ***PCI DSS and/or PA-DSS Reference*** |
|---|---|---|
| **QIR Access** | | |
| 1. Are all QIR personnel using unique accounts and passwords for each customer location? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the QIR 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 locations. | PCI DSS Requirement 8.5.1<br>PA-DSS Requirement 3.1 |
| 2. 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.<br>A response of "Yes" indicates that the QIR Employee has provided the customer with:<br>• A list of all accounts that were created by the QIR Employee, including those for the customer's use<br>• A list of all accounts used by QIR personnel<br>This includes all accounts created for the payment application, any dependent software accounts, any operating system accounts, network access accounts, etc. The QIR Employee has confidence that the customer understands how to change the passwords for all accounts created. The customer also | PCI DSS Requirement 2.1<br>PA-DSS Requirement 3.1 |

| *Item for completion in QIR Implementation Statement* | *Instruction for QIR Employee to complete* | *PCI DSS and/or PA-DSS Reference* |
|---|---|---|
| | understands how to disable or remove those accounts. | |
| **Remote Access** | | |
| 3. Is the customer aware that any remote access into their network must be configured as follows: | | |
| • Remote access to the payment application requires two-factor authentication? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the QIR Employee has confidence that the customer understands that two-factor authentication is required for any remote access to the payment application or to the customer's cardholder data environment that originates from outside the customer environment.<br>Two-factor authentication requires that two of the following authentication methods be used  in addition to a unique user ID:<br>• A password or passphrase (Something you Know)<br>• A token device or smart card (Something you Have)<br>• A biometric (Something you Are)<br>Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication. | PCI DSS Requirement 8.3<br>PA-DSS Requirement 10.1 |
| • 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.<br>A response of "Yes" indicates that the QIR Employee 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 12.3.9<br>PA-DSS Requirement 10.2.1 |
| • Remote access must be implemented securely? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the QIR Employee has confidence that the customer understands that any remote access to their network must be implemented in a secure manner, such as:<br>• Default settings in the remote access software are changed (for example, change default passwords and use unique passwords for each customer)<br>• Connections are allowed only from specific (known) IP/MAC addresses<br>• Strong authentication and complex passwords for logins are used<br>• Encrypted data transmission is enabled<br>• Account lockout after a certain number of failed login attempts is enabled<br>• Virtual Private Network ("VPN") connections are established via a | PA-DSS Requirement 10.2.3<br>PCI DSS Requirement 1.4<br>PCI DSS Requirement 5<br>PCI DSS Requirement 6.2 |

| *Item for completion in QIR Implementation Statement* | *Instruction for QIR Employee to complete* | *PCI DSS and/or PA-DSS Reference* |
|---|---|---|
| | firewall before access is allowed<br>• The logging function is enabled<br>• Access to accounts on the customer network is restricted to authorized integrator/reseller personnel<br>• Customer passwords are established according to PCI DSS Requirements<br>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 and anti-virus, be protected by a firewall, etc. | |
| 4. 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 has remote access to the customer site: | Checking the "Yes" box for question 4 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 two-factor authentication? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that all QIR personnel are required to use two-factor authentication when accessing the customer site remotely. | PCI DSS Requirement 8.3<br>PA-DSS Requirement 10.1 |
| • Is remote access to the customer network activated only when needed, access monitored when in use and immediately deactivated after use? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the customer has a process in place to activate remote access only when QIR personnel need it, monitor access while in use and to deactivate remote access immediately when it is no longer needed. | PCI DSS Requirement 12.3.9<br>PA-DSS Requirement 10.2.1 |
| • Is remote access to the customer network implemented securely? | Select "Yes" or "No" from the drop-down menu.<br>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:<br>• Default settings in the remote access software are changed (for example, change default passwords and use unique passwords for each customer)<br>• Connections are allowed only from specific (known) IP/MAC addresses<br>• Strong authentication and complex passwords for logins are used<br>• Encrypted data transmission is enabled<br>• Account lockout after a certain number of failed login attempts is enabled | PCI DSS Requirement 1.4<br>PCI DSS Requirement 5<br>PCI DSS Requirement 6.2<br>PA-DSS Requirement 10.2.3 |

| ***Item for completion in QIR Implementation Statement*** | | ***Instruction for QIR Employee to complete*** | ***PCI DSS and/or PA-DSS Reference*** |
|---|---|---|---|
| | | • Virtual Private Network ("VPN") connections are established via a firewall before access is allowed<br>• The logging function is enabled<br>• Access to accounts on the customer network is restricted to authorized integrator/reseller personnel<br>• Customer passwords are established according to PCI DSS Requirements<br>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 and anti-virus, be protected by a firewall, etc. | |
| □ | **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 question 4 indicates that the QIR Employee 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 will not be configuring the customer's remote access. | |
| **Network configuration** | | | |
| **5.** Are any external connections required by the payment application? | | | |
| *Check either the "Yes" or "No" box. If the "Yes" box is checked, the applicable bullet points must also be answered:* | | | |
| □ | **Yes.** The payment application requires external connections: | Checking the "Yes" box for question 5 indicates that the QIR Employee is aware that one or more external connections are required by the payment application. | |
| | • Is the customer aware of all connections required by the payment application? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the QIR Employee has confidence that the customer is aware of all external connections to/from the payment application.<br>For example, the customer should be aware of the following for each external connection to/from the payment application:<br>• The purpose of the connection<br>• The external end-point of the connection (for example, company is the connection going to)<br>• Whether any cardholder data is being transmitted over the connection<br>• How the connection is secured to protect sensitive data | PCI DSS Requirement 1.1.2 |
| | • Is the customer aware they must use a firewall that allows only required | Select "Yes" or "No" from the drop-down menu. | PCI DSS Requirement 1 |

| ***Item for completion in QIR Implementation Statement*** | ***Instruction for QIR Employee to complete*** | ***PCI DSS and/or PA-DSS Reference*** |
|---|---|---|
| ports on both inbound and outbound connections? | A response of “Yes” indicates that the QIR Employee has confidence that the customer understands that they must implement and configure a firewall to restrict inbound and outbound traffic so that only that which is necessary for their particular environment is allowed in or out of their network.<br>Leaving unnecessary ports open can result in unsecured points of entry into the customer’s network for malicious users to exploit. | |
| • Is the customer aware that external connections to/from the payment application should only be permitted to specific (known) IP addresses? | Select “Yes” or “No” from the drop-down menu.<br>A response of “Yes” indicates that the QIR Employee has confidence that the customer understands that any external connections to or from the payment application are to pre-defined, specific IP addresses. The firewall should be configured to ensure the payment application can only communicate with trusted external sources. | PCI DSS Requirement 1.2.1 |
| • Is the customer aware they should enable logging on the firewall? | Select “Yes” or “No” from the drop-down menu.<br>A response of “Yes” indicates that the QIR Employee has confidence that the customer understands that they must enable logging on the firewall.<br>Firewall logs should be backed up to a centralized log server or media and secured from unauthorized access. | PCI DSS Requirement 10 |
| □ **No.** No external connections were required by the payment application. | Checking the “No” box for question 5 indicates that there are no external connections to or from the payment application. | |
| **Sensitive Authentication Data (SAD)** | | |
| 6. Is the application configured to ensure that sensitive authentication data (including full track data, card verification codes/values and PIN or PIN block) is not stored after authorization, even if encrypted? | Select “Yes” or “No” from the drop-down menu.<br>A response of “Yes” indicates that the QIR Employee has confirmed that the application is configured in a manner that prevents any sensitive authentication data from being retained once authorization of a transaction has been completed.<br>This may be achieved as follows:<br>• The application does not have any capability to store SAD, and does not provide any configuration option that might result in storage of any SAD post-authorization, or<br>• If the application does have an option that permits SAD to be stored post-authorization, all such options are disabled. | PA-DSS Requirement 1.1<br>PCI DSS Requirement 3.2 |
| **Troubleshooting and Maintenance** | | |
| 7. Does the QIR provide services to the customer that could potentially result in the collection of cardholder data and/or sensitive authentication data (for | | |

| ***Item for completion in QIR Implementation Statement*** | ***Instruction for QIR Employee to complete*** | ***PCI DSS and/or PA-DSS Reference*** |
|---|---|---|
| example, for troubleshooting or debugging purposes)? | | |
| *Check either the "Yes" or "No" box. If the "Yes" box is checked, the applicable bullet points must also be answered:* | | |
| ☐ **Yes.** The QIR provides services to the customer that could potentially result in the collection of cardholder data and/or sensitive authentication data. | Checking the "Yes" box for question 7 indicates that services provided by the QIR to the customer could possibly collect cardholder data or sensitive authentication data.<br>***Note:*** *if the QIR collects cardholder data and/or sensitive authentication data on their own systems, the QIR would be responsible for securing the data according to all applicable PCI DSS requirements.* | |
| • Is sensitive authentication data collected only when needed, and collection limited to only the amount needed, to solve a specific problem? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that sensitive authentication data is only ever collected as follows:<br>• Sensitive authentication data is only collected when a specific problem is identified that requires temporary collection of sensitive authentication data<br>• Sensitive authentication data is only collected during specific times as needed to solve that specific problem<br>• The minimum amount of sensitive authentication data needed to solve the specific problem is collected<br>If the application is temporarily configured to capture SAD for troubleshooting or debugging purposes, the application must be returned to its usual secure configuration (that is, this configuration option must be returned to a disabled state) immediately upon completion of the necessary data capture. | PCI DSS Requirement 3.1<br>PA-DSS Requirement 1.1.5 |
| • Is sensitive authentication data stored encrypted in a secure location with limited access? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that sensitive authentication data  is always handled as follows:<br>• Sensitive authentication data is stored only in specific, known locations<br>• Access to the sensitive authentication data is limited to specific individuals requiring access to solve that specific problem<br>• Sensitive authentication data is stored encrypted with strong cryptography | PA-DSS Requirement 1.1.5 |
| • Is sensitive authentication data securely deleted immediately after use? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that sensitive authentication data is securely deleted immediately once it is no longer needed for that specific problem, and | PCI DSS Requirement 3.2<br>PA-DSS Requirement 1.1.5 |

| *Item for completion in QIR Implementation Statement* | *Instruction for QIR Employee to complete* | *PCI DSS and/or PA-DSS Reference* |
|---|---|---|
| | is deleted in accordance with industry-accepted standards for secure deletion. (For example, using a secure wipe program or other method that ensures that the data is can never be retrieved.) | |
| • Is PAN rendered unreadable when stored? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that any Primary Account Numbers are rendered unreadable when stored using one of the following approaches:<br>• One-way hashes based on strong cryptography (hash must be of the entire PAN)<br>• Truncation (hashing cannot be used to replace the truncated segment of PAN)<br>• Index tokens and pads (pads must be securely stored)<br>• Strong cryptography with associated key-management processes and procedures | PCI DSS Requirement 3.4<br>PA-DSS Requirement 2.3 |
| □ **No.** The QIR does not provide any service to the customer that could result in collection of cardholder data and/or sensitive authentication data. | Checking the "No" box for question 7 indicates that no services provided by the QIR could result in the QIR collecting PAN or SAD. | |
| **Protection of Cardholder Data** | | |
| 8. Does the application store cardholder data? | | |
| *Check either the "Yes" or "No" box. If the "Yes" box is checked, the applicable bullet points must also be answered:* | | |
| □ **Yes.** The application does store cardholder data: | Checking the "Yes" box for question 8 indicates that the payment application stores cardholder data (CHD). Cardholder data, as defined in the PCI DSS Glossary of Terms, Abbreviations and Acronyms, consists, at a minimum, of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. | |
| • Is PAN rendered unreadable anywhere it is stored? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the QIR Employee has confirmed that the PAN is unreadable anywhere it is stored, including:<br>• Any data repositories created or generated by the application<br>• Any files generated by the application for export or use outside the application (including those generated on removable media)<br>• Any audit logs created or generated by the application<br>PAN can be rendered unreadable, as instructed in the *PA-DSS* | PCI DSS Requirement 3.4<br>PA-DSS Requirement 2.3 |

| *Item for completion in QIR Implementation Statement* | | *Instruction for QIR Employee to complete* | *PCI DSS and/or PA-DSS Reference* |
|---|---|---|---|
| | | *Implementation Guide*, by using any of the following approaches:<br>• One-way hashes based on strong cryptography (hash must be of the entire PAN)<br>• Truncation (hashing cannot be used to replace the truncated segment of PAN)<br>• Index tokens and pads (pads must be securely stored)<br>• Strong cryptography with associated key-management processes and procedures | |
| | • Is the customer aware they must securely manage all cryptographic keys? | Select “Yes” or “No” from the drop-down menu.<br>A response of “Yes” indicates that the QIR Employee has confidence that the customer understands that all cryptographic keys need to be securely managed.  Cryptographic keys can include those used by the payment application, by any dependent software, such as databases or other applications,  or by operating systems.<br>All cryptographic keys need to be securely stored in the fewest possible locations, with data-encrypting keys stored separately from key-encrypting keys and key encrypting keys need to be at least as strong as the data encrypting keys they protect.   Access to keys should be restricted to the fewest number of custodians necessary. | PCI DSS Requirements 3.5 and 3.6<br>PA-DSS Requirements 2.4 and 2.5 |
| | • Is the customer aware they must not store cardholder data on Internet-accessible systems? | Select “Yes” or “No” from the drop-down menu.<br>A response of “Yes” indicates that the QIR Employee has confidence that the customer understands that cardholder data should not be stored on Internet-accessible systems and that this understanding includes:<br>• Configuring the payment application to use a DMZ to separate the Internet from systems storing cardholder data<br>• Configuring the firewall to open only required ports in order to communicate across two network zones<br>For example, a database containing cardholder data must not be on a web server. Cardholder data should be stored on an internal segment of the network, segregated from the DMZ and any public networks. | PCI DSS Requirement 1.3.7<br>PA-DSS Requirement 9.1 |
| ☐ | **No.** The application does not store cardholder data. | Checking the “No” box for question 8 indicates that the payment application does not store cardholder data anywhere, including in:<br>• Any data repositories created or generated by the application<br>• Any files generated by the application for export or use outside the application (including those generated on removable media) | |

| *Item for completion in QIR Implementation Statement* | *Instruction for QIR Employee to complete* | *PCI DSS and/or PA-DSS Reference* |
|---|---|---|
| | • Any audit logs created or generated by the application | |
| 9. Is the customer aware that cardholder data must be protected with strong cryptography if sent over public networks or end-user messaging technologies? | Select “Yes” or “No” from the drop-down menu.<br>A response of “Yes” indicates that the QIR Employee has confidence that the customer understands that strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) must be established and maintained when transmitting cardholder data over public networks, including the following:<br>▪ Only trusted keys and certificates are accepted<br>▪ The protocol in use only supports secure versions or configurations<br>▪ The encryption strength is appropriate for the encryption methodology in use<br>Examples of public networks include but are not limited to:<br>• The Internet<br>• Wireless technologies, including but not limited to 802.11 and Bluetooth<br>• Cellular technologies, for example, Global System for Mobile Communications (GSM), Code division multiple access (CDMA)<br>• General Packet Radio Service (GPRS)<br>• Satellite communications<br>A response of “Yes” also indicates that the QIR Employee has confidence that the customer understands that PAN data must be made unreadable (for example, with strong cryptography) if sent with end-user messaging technologies such as e-mail, instant messaging, chat, etc. | PCI DSS Requirements 4.1 and 4.2<br>PA-DSS Requirements 11.1 and 11.2 |
| 10. Is the customer aware that, if available, encryption of cardholder data transmissions from the customer to back-end processors and/or acquirer is recommended, even for private connections? | Select “Yes” or “No” from the drop-down menu.<br>A response of “Yes” indicates that the QIR Employee has confidence that the customer understands that, if encryption is available, cardholder data transmissions from the customer to back-end processors or to the acquirer should be encrypted, even when sent over private connections. An example of a private network connection may be a dedicated T-1 line. Encrypting all transmissions of cardholder data, even when sent over private connections, will help to minimize the risk of a cardholder data compromise while in transit. | |
| 11. Is the customer aware that any non-console administrative access to systems in their CDE, including the payment application, must be secured? | Select “Yes” or “No” from the drop-down menu.<br>A response of “Yes” indicates that the QIR Employee has confidence that the customer understands that they must implement and use strong cryptography (such as SSH, VPN, or SSL/TLS) for any non-console administrative access to | PCI DSS Requirement 2.3<br>PA-DSS Requirement 12.2 |

| *Item for completion in QIR Implementation Statement* | *Instruction for QIR Employee to complete* | *PCI DSS and/or PA-DSS Reference* |
|---|---|---|
| | the payment application or its underlying system.<br>If administrative access is needed to any other system in the cardholder data environment, it should also be secured with strong cryptography.<br>***Note:*** *Telnet or rlogin must never be used for administrative access to the CDE.* | |
| **Accounts and Passwords** | | |
| 12. 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.<br>A response of "Yes" indicates that all passwords have been changed for:<br>• All payment application user default accounts, and<br>• All payment application administrative default accounts.<br>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.**<br>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.<br>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<br>PA-DSS Requirement 3.1 |
| 13. Is strong authentication configured for all application administrative accounts and for all application accounts with access to cardholder data? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the QIR Employee has confirmed that strong authentication is configured for:<br>• All application accounts with administrative access, and<br>• All application accounts with access to cardholder data.<br>This includes all credentials which 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:<br>• Not using group, shared, or generic accounts and passwords, or other authentication methods | PCI DSS Requirements 8.5, 8.2.3 – 8.2.5, 8.1.6 – 8.1.8<br>PA-DSS Requirements 3.1.5 - 3.1.11 |

| *Item for completion in QIR Implementation Statement* | *Instruction for QIR Employee to complete* | *PCI DSS and/or PA-DSS Reference* |
|---|---|---|
| | • Changing user passwords at least every 90 days<br>• Requiring a minimum password length of at least seven characters<br>• Using passwords containing both numeric and alphabetic characters<br>• 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<br>• Locking out the user ID after not more than six attempts<br>• Setting the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID<br>• Requiring users to re-authenticate after 15 minutes of an idle session<br>Strong credentials need to be in place by the completion of the application's installation and for subsequent changes after installation.<br>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. | |
| 14. 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.<br>A response of "Yes" indicates that the QIR Employee 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 13 above (per PCI DSS Requirements 8.5.8 – 8.5.15). | PCI DSS Requirement 8.1<br>PA-DSS Requirement 3.2 |
| 15. Is the customer aware that, for all accounts used by operating systems, security software, applications, systems, POS terminals, etc.:<br>a. All vendor-supplied defaults should be changed, and<br>b. All unnecessary default accounts should be removed or disabled? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the QIR Employee 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<br>PA-DSS Requirement 3.2 |
| **Logging** | | |
| 16. Is payment application logging enabled? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the QIR Employee has confirmed that payment application logging is enabled and active, and that the payment application audit trails are recording the appropriate events and entries. | PCI DSS Requirement 10.2 and 10.3<br>PA-DSS Requirements 4.2, 4.3 and 4.4 |

| *Item for completion in QIR Implementation Statement* | *Instruction for QIR Employee to complete* | *PCI DSS and/or PA-DSS Reference* |
|---|---|---|
| | Events that must be logged are defined in PCI DSS Requirement 10.2 and 10.3, and include:<br>• All individual accesses to cardholder data from the application<br>• All actions taken by any individual with administrative privileges as assigned in the application<br>• Access to application audit trails managed by or within the application<br>• Invalid logical access attempts<br>• Use of and changes to the application's identification and authentication mechanisms (including but not limited to creation of new accounts, elevation of privileges, etc.) and all changes, additions, deletions to application accounts with root or administrative privileges<br>• Initialization of the application audit logs<br>• Creation and deletion of system-level objects within or by the application<br>For each event logged, the following information must be recorded:<br>• User identification<br>• Type of event<br>• Date and time<br>• Success or failure indication<br>• Origination of event<br>• Identity or name of affected data, system component or resource<br>If the application is dependent on underlying software, such as databases or operating systems, to perform some or all logging, these logs must also be enabled and configured to record the appropriate events and entries.<br>All logs should be able to be assimilated into a centralized log server. | |
| 17. Is the customer aware that logs should not be disabled and doing so will result in non-compliance with PCI DSS? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the QIR Employee has confidence that the customer understands that PCI DSS requires that logs are enabled at all times, and that disabling logs will result in non-compliance | PCI DSS Requirement 10.1<br>PA-DSS Requirement 4.1 |
| **Wireless** | | |
| 18. Does the payment application use wireless technology? | | |

*Check either the "Yes" or "No" box. If the "Yes" box is checked, the applicable bullet points must also be answered:*

| ***Item for completion in QIR Implementation Statement*** | | ***Instruction for QIR Employee to complete*** | ***PCI DSS and/or PA-DSS Reference*** |
|---|---|---|---|
| □ | **Yes.** The payment application uses wireless technology: | Checking the "Yes" box for question 17 indicates that the payment application uses wireless technology, or that the customer has or will implement the payment application in an environment that uses wireless technology. | |
| | • Is the customer aware that all wireless vendor defaults must be changed? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the QIR Employee has confidence that the customer understands that they must change all wireless vendor defaults. This includes changing:<br>• Wireless encryption keys<br>• SNMP community strings<br>• Passwords or passphrases on access points<br>• Other security-related defaults | PCI DSS Requirement 2.1.1<br>PA-DSS Requirement 6.1 |
| | • Is the customer aware they must install and properly configure a firewall between any wireless networks and systems in the cardholder data environment? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the QIR Employee has confidence that the customer understands they must install and configure a firewall to separate the wireless network from the cardholder environment. The configuration must ensure that traffic between the wireless network and the cardholder data environment is limited to that necessary for business purposes. | PCI DSS Requirement 1.2.3<br>PA-DSS Requirement 6.1 |
| | • Is the customer aware they must implement strong encryption for authentication and transmission of cardholder data over wireless networks? | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the QIR Employee has confidence that the customer understands they must ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices to implement strong encryption for authentication and transmission. An example of an industry best practice for strong encryption is IEEE 802.11.i. | PCI DSS Requirement 4.1.1<br>PA-DSS Requirement 6.2 |
| □ | **No.** The payment application does not use wireless technology. | Checking the "No" box for question 17 indicates that the payment application does not use wireless technology nor will the customer be implementing the payment application into a wireless environment. | |
| **Patching** | | | |
| 19. Have the latest vendor-supplied security patches and updates been applied to all software installed by the QIR Employee, including the payment application? | | Select "Yes" or "No" from the drop-down menu.<br>A response of "Yes" indicates that the QIR Employee 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 Employee such as dependent software or operating systems. | PCI DSS Requirement 6.1<br>PA-DSS Requirement 7.2 |

| ***Item for completion in QIR Implementation Statement*** | ***Instruction for QIR Employee to complete*** | ***PCI DSS and/or PA-DSS Reference*** |
|---|---|---|
| | If dependent or underlying software, such as databases or operating systems, are provided as part of the Qualified Installation, the QIR Employee should configure the operating system and underlying software in accordance with all applicable PCI DSS requirements. | |
| 20. 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 Employee 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 6.1 |

## *Part 3 QIR Employee Additional Observations*

Part 3, QIR Employee Additional Observations, has several purposes. The first is to provide details of all responses where the QIR Employee selected *"No – Details provided in Part 3"*. Each "No" response must be explained in its own row. Secondly, the QIR Employee must record any potential PCI DSS compliance issues identified. Thirdly, the QIR Employee should include any other observations they feel the customer should be aware of regarding the Qualified Installation.

If aspects of the installation were performed by parties other than the QIR (for example, the customer or other third party), the QIR Employee 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: | Records any observations that the QIR Employee wishes to bring to a customer's attention, including any potential PCI DSS compliance issues, 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 Implementation Statement, record the applicable question number here. |
| Potential PCI DSS compliance issue?: | If the QIR Employee feels that the observation could possibly effect or have an impact on the customer's PCI DSS compliance, check "Yes". If the observation is not relevant to any PCI DSS requirement, check "No".<br>Note: It is not the QIR'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. |

Some examples are provided below. Note: these are examples only and are provided to assist the QIR Employee understand how the table is to be used to record their observations.

| Observation # | Observation Details | Applicable subject and question number from Part 2 | Potential PCI DSS compliance issue? | | 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 18 | ☒ | ☐ | PCI DSS Requirements 6.1 and 6.2 |
| 2 | There does not appear to be a firewall installed to control traffic from the wireless network to the cardholder data environment. | Wireless – Question 17 | ☒ | ☐ | PCI DSS Requirement 1.2.3 |
| 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 Employee may adjust column width and add/remove rows as needed to record all their observations. However, the QIR Employee must not remove any columns or change column headings.*