Payment Card Industry (PCI)

Payment Application Data Security Standard

ROV Reporting Instructions
for PA-DSS v2.0

March 2012

Document Changes

Date	Document Version	Description	Pages
March 2012	1.0	To introduce PA-DSS ROV Reporting Instructions for PA-DSS version 2.0.	

Table of Contents

Introduction

The Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS) is for software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.

The *PA-DSS Requirements and Security Assessment Procedures* includes a template for creating and completing a ROV. This document, *ROV Reporting Instructions for PA-DSS v2.0*, provides additional instructions and guidance for PA-QSAs to ensure that a consistent level of reporting is maintained.

All details relevant to the PA-QSA's findings should be clearly identified and documented in the appropriate place within the ROV. The information recorded in the ROV must ultimately support the PA-QSA's findings of "in place" or "not in place" for each PA-DSS Requirement and Testing Procedure.

Report on Validation Content

At a high level, the ROV provides a comprehensive summary of testing activities performed and information collected during the assessment. The information contained in a ROV must provide enough detail and coverage to verify that the payment application is compliant with all PA-DSS requirements. The assessor should clearly describe how the validation activities were performed and how the resultant findings were reached for each section of the ROV.

As defined in the *PA-DSS Requirements and Security Assessment Procedures*, the ROV includes the following sections:

- Section 1: Description of Scope of Review
- Section 2: Executive Summary
- Section 3: Findings and Observations
- Section 4: Contact Information and Report Date

Section 1, "Description of Scope of Review," contains information related to how the PA-DSS assessment was scoped. Guidance on scoping is contained in the PA-DSS standard under the section titled "Scope of PA-DSS." The assessor will provide information on what was included as well as excluded from the assessment. Other details to be included in this section are the timeframe in which the validation occurred, the version of the PA-DSS utilized in conducting the review, as well as a listing of documentation reviewed.

Section 2, "Executive Summary," contains a high-level overview of the application environment undergoing the review. The information provided in this section should give the reader an overall understanding of the application and how the application is typically implemented in a customer environment.

If these first two sections are not thoroughly and accurately completed, the assessment findings will not have proper context.

Section 3, "Findings and Observations," contains the assessor's findings for each PA-DSS Requirement and Testing Procedure as well as information that supports and justifies each finding. The information provided in "Findings and Observations" summarizes how the testing

procedures were performed and the findings achieved. This section includes all thirteen PA-DSS requirements. All findings and observations should be supported by and consistent with the information in Sections 1 and 2.

Section 4, "Contact Information and Report Date," contains the contact information for the application vendor, the PA-QSA conducting the assessment, and the primary contact at the PA-QSA organization responsible for all PA-QSA quality assurance activities.

Assessor Documentation

A PA-DSS compliance assessment involves thorough testing and assessment activities, from which the assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities, including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the course of the assessment to support the assessor's findings. The assessor's work papers should be retained and protected in accordance with PCI SSC program requirements.

Not all the information in the work papers will be included in the ROV. The ROV is effectively a summary of all the evidence collected, and while the information presented in the ROV is derived from the work papers, the ROV itself should not be a replication of every piece of evidence collected.

How to Use the ROV Reporting Instructions

These ROV Reporting Instructions identify the information and level of detail to be recorded in each section of the ROV.

Description of Scope of Review, Executive Summary, Contact Information and Report Date (ROV Sections 1, 2, 4)

This section provides reporting instructions for all sections of the ROV and is presented in two columns:

- **ROV Section (PA-DSS Template) –** Corresponds to the ROV template as provided in the "Instructions and Content for Report on Validation" section of the *PA-DSS Requirements and Testing Procedures*.
- **ROV Reporting Details –** Outlines the information and level of detail to be provided for each item in the ROV template.

Findings and Observations – PA-DSS Requirements (ROV Section 3)

This section contains instructions for reporting findings and observations for PA-DSS requirements, and is presented as follows:

- **PA-DSS Requirements and Testing Procedures –** Corresponds to the Requirements and Testing Procedures from the PA-DSS.
- **ROV Reporting Details –** Outlines the information and level of detail to be provided for each testing procedure. Note that the format of responses in a ROV is not expected to mirror the format in the Reporting Details column. The information provided in the Reporting Details column is bulleted and indexed in this document for ease of readability. It is not intended that PA-QSAs follow this format when writing a ROV. However, PA-QSAs should ensure that they include all the required information in each response.
- **Reporting Methodology** – Identifies which methods used by the PA-QSA to collect the requisite evidence are to be reported in the ROV for each testing procedure. Note that the methods identified for inclusion in the ROV may not be all-inclusive of the methods used during an actual assessment. The PA-QSA may need to employ additional methods during the assessment to reach a finding of "in place" or "not in place." Where additional methods are used to validate a finding, the PA-QSA should also report those details in the ROV.

Reporting Methodology

The reporting methodologies to be included for each testing procedure are identified with a check mark (✓) in the Reporting Methodology column. The different reporting methodologies are described in the following table.

Reporting Methodology	Description
Observe system settings, configurations	▪ PA-QSA observes actual application and/or underlying system components. ▪ May include different configuration files, settings, or other parameters on each system observed. ▪ Observation may require assistance from appropriate personnel (e.g., developers or support personnel). ▪ Observation verifies that such parameters are set to produce a specified outcome.
Document reviews	▪ PA-QSA reviews documentation provided by the assessed entity. ▪ Documentation may include the application vendor's Implementation Guide. ▪ Documentation may also include, but is not limited to: training materials, application manuals, policies, procedures, processes, configuration standards, network diagrams, other vendor documentation, reports, logs, audit trails, and industry standards and best practices. ▪ Reviews of documentation verify the inclusion of items specified in the requirement/testing procedure. ▪ Reviews of the payment application Implementation Guide verify that the included items are relevant to the specific application and provide accurate and effective configuration instructions (where applicable).
Interviews with personnel	▪ PA-QSA interviews person or persons as appropriate for the requirement/testing procedure. ▪ Results of interviews may demonstrate that an action has or has not been performed, or that the interviewee has particular knowledge or understanding.
Observe process, action, state	▪ PA-QSA observations may include, but are not limited to: • Descriptions of testing methods used by the PA-QSA (for example, penetration testing techniques, forensic tools, etc) • Actions of people performing or not performing a task or procedures • Behavior of applications or system components in response to an action • Communications and network traffic • Environmental conditions, including physical controls • Walk-through of a process or procedure to verify the steps being performed • Other evidence or output resulting from a task or action ▪ Observation may require assistance from appropriate personnel. ▪ Observation verifies a specified result or outcome.
Identify sample	▪ PA-QSA selects a representative sample as appropriate for the requirement/testing procedure. ▪ Justification of sample provides assurance that controls are uniformly and consistently applied to all items.

ROV Reporting Details

Instructions provided in the Reporting Details column correspond with one or more checked columns in the Reporting Methodologies column, for each requirement/testing procedure. Guidance for understanding the instructions used in the Reporting Details column is provided below.

- **Example instruction: "Describe how system configurations…"**
  - Identify the files, parameters or settings that were examined (for example, boot configuration files, account permissions, access control lists, rule sets, connection setting, application access policy settings, startup configuration files, etc.) on each system component.
  - This is not intended to be a list of file names. However, the description should include a suitable amount of detail to provide assurance that the appropriate files were reviewed.
  - Generic phrases such as "system settings" or "system configurations" are not sufficient.
  - Describe how the observed files or settings satisfy the requirement/testing procedure.
- **Example instruction: "Identify the document …"**
  - Identify the reviewed document by name. *(**Note**: The term "document" may refer to multiple documents or documentation sets.)*
  - Ensure all identified documents are also included in the List of Documentation Reviewed, under "Description of Scope of Review" (Section 1).
  - Describe how the information contained within the reviewed document satisfies the requirement/testing procedure.
  - The assessor should confirm that the documented processes, policies, or procedures are in place and being followed, and not merely that a document exists.
  - By identifying a document in the ROV, the assessor is attesting that the processes, policies, procedures, or practices contained in that document are sound.
  - For Implementation Guide requirements, the assessor should confirm that the information provided is accurate and clearly describes how to configure the payment application to meet the particular requirement. The assessor should also verify that performing the documented instructions results in the requirement being met. Please see the section "PA-DSS Implementation Guide" below, for further guidance.
- **Example instruction: "Identify the personnel interviewed…"**
  - Identify the roles or positions of the personnel interviewed.
  - If the testing procedure identifies personnel in a specific position to be interviewed, ensure that personnel in those positions are in fact interviewed.
  - If a specific position doesn't exist, it is the assessor's responsibility to identify the appropriate personnel to interview. Explain how interviews with the identified personnel meet the intent of the specified position. For example, if a testing procedure includes interviewing software developers, the PA-QSA should ensure that they interview personnel who perform software development as

part of their job function. Note that such personnel may not have the exact title "Software Developer", but their title may still indicate that they are in fact the appropriate personnel to interview. If the job title does not reflect the applicable role, the PA-QSA should verify that the person interviewed does in fact perform the role applicable to the testing procedure.

- Summarize the relevant details discussed during the interview and describe how the requirement/testing procedure is satisfied.
- Ensure all interviewed persons are also included in the List of Individuals Interviewed, under "Description of Scope of Review" (Section 1).

- **Example instruction: "Describe how it was observed…"**
  - Identify and describe the process, procedure, action, or state that was observed.
  - Identify any personnel or system components that were part of the observation.
  - Describe any situational or environmental factors relevant to the observation.
  - Describe how the observations provide assurance that the requirement/testing procedure is satisfied.

- **Example instruction: "Identify all instances where…"**
  - Identify the circumstances applicable to the occurrence of a particular event.

- **Example instruction: "Identify the sample of…"**
  - Identify the number and type of items included in each sample—for example, 20 troubleshooting requests or 5 key custodian forms.
  - It is not necessary to identify the names of every sampled system component in the ROV. However, assessors may provide a list if it improves clarity or better explains the findings for some applications. Irrespective of whether system component names are recorded in the ROV, the PA-QSA must maintain a detailed record of each sampled component in their work papers.
  - Samples must be representative of the entire payment application environment.
  - The types of items in the sample must be appropriate for the requirement/testing procedure.

- **Example instruction: "Briefly describe how the PA-DSS Implementation Guide includes…"**
  - Summarize how the PA-DSS Implementation Guide addresses the required controls.
  - It is not intended that sections of the PA-DSS Implementation Guide be copied into the ROV.
  - The assessor must also validate that information provided in the PA-DSS Implementation Guide is accurate and effective (for example, instructions work correctly, file locations are accurately identified, etc.)

PA-DSS Implementation Guide

As defined in the *PA-DSS Requirements and Security Assessment Procedures*, payment application vendors are required to provide a PA-DSS Implementation Guide to:

- Instruct their customers and resellers/integrators on secure product implementation,
- Document the secure configuration specifics required throughout the PA-DSS, and
- Clearly delineate vendor, reseller/integrator, and customer responsibilities for meeting PCI DSS requirements.

The Implementation Guide must be specific to each application and provide instructions on how to implement the application in a PCI DSS compliant manner. It is not sufficient for the Implementation Guide to simply reiterate requirements from the PA-DSS and PCI DSS.

As part of the assessment, the PA-QSA must utilize the Implementation Guide during installation and testing of the application to verify that the Implementation Guide contains proper instructions and guidance for customers and resellers/integrators to install, configure, and maintain the payment application in a PCI DSS compliant manner. For requirements that specifically include an Implementation Guide component, the assessor is required to verify that configuration instructions are accurate and effective, such that performing the instructions results in the requirement being met.

"Not Applicable" Requirements

If a PA-DSS Requirement or Testing Procedure is determined to be "not applicable" (N/A), this should be clearly identified in the "In Place" column.

Findings of "in place" due to the control being N/A must include a detailed description of what was tested and/or observed to determine that the control is not applicable for the given application.

General Guidance and Best Practices

Critical Test Procedures

PCI SSC has defined a number of critical test procedures which have been identified as particularly critical to the protection of cardholder data in PA-DSS compliant payment applications. These critical test procedures address control areas that have historically been targeted by attackers attempting to compromise payment applications, including; sensitive authentication data, remote access, default passwords, secure storage and transmission of PAN, logging, and wireless. The PA-DSS requirements addressing critical test procedures for these control areas are identified in the table below.

PA-QSAs should pay careful attention to ensure that all critical test procedures are properly assessed and appropriately documented in the ROV.

Critical Areas	PA-DSS Requirements
Sensitive Authentication Data	Requirement 1
Remote Access	Requirement 10, Requirement 12
Default Passwords	Requirement 3, Requirement 5.4
Secure storage and transmission of PAN	Requirements 2.3 – 2.6, Requirement 11
Logging	Requirement 4
Wireless	Requirement 6

Note: *These critical test procedures are provided for additional guidance and informational purposes only. PA-QSAs must ensure that* ***all*** *PA-DSS testing procedures are thoroughly assessed and that all findings are properly documented in the ROV.*

Do's and Don'ts

DO:

- Follow the ROV template provided in the *PA-DSS Requirements and Security Assessment Procedures*.
- Complete all sections in the order specified, with consistent numbering, titles, and headings.
- Read and understand the intent of each requirement and testing procedure.
- Provide a response for every testing procedure.
- Provide sufficient detail and information to demonstrate a finding of "in place".
- Describe how a Requirement was verified, not just that it was verified.
- Describe what was performed for each testing procedure.
- Ensure the response addresses all parts of the testing procedure.
- Ensure the response covers all applicable application and/or system components.
- Ensure the lists of documentation and interviewees in the "Description of Scope of Review" section are complete and include all such items referenced in the body of the ROV.
- Perform an internal quality assurance review of the ROV for clarity, accuracy, and quality.

DON'T:

- Don't report items in the "In Place" column unless they have been verified as being "in place".
- Don't include forward-looking statements or project plans in the "In Place" column.
- Don't simply repeat or echo the testing procedure in the response.
- Don't copy responses from one testing procedure to another.
- Don't copy responses from previous assessments.
- Don't cross-reference between responses.
- Don't include information that is not relevant to the assessment or individual findings.

ROV Reporting Instructions for PA-DSS v2.0

ROV Section (PA-DSS) Template	ROV Reporting Details
1. Description of Scope of Review	

▪ Describe scope of review coverage, per the "Scope of PA-DSS" section	• Identify the application and all application components included in this review.
	• Provide a full description of the application including:
	  ○ The type of application (for example, POS terminal, payment switch, shopping cart, kiosk, etc.)
	  ○ The purpose and use of the payment application, for example:
	  – Types of transactions
	  – Whether the application is designed for specific payment acceptance channels (for example, card present and card not present)
	  – How the application stores, process, or transmits cardholder data as part of authorization or settlement
	  – How the payment application is sold, distributed, or licensed to third parties.
	  – Whether the payment application is provided in modules, and if so, which modules perform payment functions
	  – Whether the application is part of a payment application suite
	• Describe how PA-DSS is applicable to this application, per the "Scope of PA-DSS" section.

	• Identify the payment application functionality that was assessed, including but not limited to:
	  ○ End-to-end payment functions (authorization and settlement)
	  ○ Input and output
	  ○ Error conditions
	  ○ Interfaces and connections to other files, systems, and/or payment applications or application components
	  ○ All cardholder data flows
	  ○ Encryption mechanisms
	  ○ Authentication mechanisms
	  ○ Other functions of the application relevant to the protection of cardholder data
	• Identify any functionality of the payment application that was not included in the assessment, and explain why it was excluded.

ROV Section (PA-DSS) Template	ROV Reporting Details

	• Describe how the Implementation Guide was confirmed to include guidance for customers and resellers/integrators to ensure that:
	  ○ Customer is clearly instructed how to implement the payment application in a PCI DSS compliant manner and
	  ○ Customer is clearly instructed that certain payment application and environment settings may prohibit their PCI DSS compliance
	  ○ Appropriate guidance is provided even when a specific setting:
	  – Cannot be controlled by the payment application vendor once the application is installed by the customer or
	  – Is the responsibility of the customer, not the payment application vendor

	• Identify all tools used by or within the payment application to access and/or view cardholder data (reporting tools, logging tools, etc.)

– Timeframe of validation	• Describe the timeframe during which the application was validated, including :
	  ○ The total time taken to complete the overall assessment (start date to completion date)
	  ○ Actual time the assessor spent performing assessment activities (including Lab time)

– PA-DSS version used for the assessment	• Identify the version of the *PA-DSS Requirements and Security Assessment Procedures* which was used for the assessment.

– List of documentation reviewed	• Identify and list each document cited in the Findings and Observations. Include the following:
	  ○ Document name
	  ○ Brief description of document purpose
	  ○ Document date

– List of individuals interviewed	• Identify and list the individuals interviewed. Include the following:
	  ○ The individual's name
	  ○ The individual's organization
	  ○ The individual's job title
	  ○ A summary of the topics covered

2. Executive Summary	
▪ Product Name	• Identify the full name of the application being assessed.
▪ Product Version and related platforms covered	• Identify the version of the product being assessed. *(Only one version can be included per submission)* • Identify all platforms that this application version was tested on during this assessment. Include details of the underlying hardware architectures (for example, mainframe, client-server, clusters, virtualized environments, hardware terminals, etc.), as well as user interfaces, programming languages, application frameworks, etc.

ROV Section (PA-DSS) Template	ROV Reporting Details
▪ List of resellers and/or integrators for this product	• Provide a full list of all resellers and/or integrators for this product
▪ Operating system(s) with which the payment application was tested	• Identify and list all operating system (s) with which the payment application was tested in this assessment. Include specific versions or service pack level, as applicable.
▪ Database software used or supported by the payment application	• Identify and list all databases with which the payment application was tested in this assessment. Include specific versions, as applicable.
▪ Brief description of the payment application/family of products (2-3 sentences)	• Provide a description of the payment application, including a description of the family of products, if the application is part of a suite or is provided in modules. • If the payment application is part of a larger suite of applications, identify any other modules or products in the application suite which were tested with the payment application.
▪ Network diagram of a typical implementation of the payment application (not necessarily a specific implementation at a customer's site) that includes, at high level:	• Provide one or more simple, high level diagrams(s) showing the overall architecture of the environment for a typical implementation. The diagrams should identify all relevant systems and the relationship between them. • Ensure the diagram(s) are clearly labeled and include the following:
– Connections into and out of a customer's network	○ All connections into and out of the network ○ All connections between the payment application and other applications, systems, networks or zones
– Components within the customer's network, including POS devices, systems, databases, and web servers as applicable	○ All critical components and systems, as well as their locations and the boundaries between them, including POS devices, systems, databases, web servers, and other components as applicable
– Other necessary payment application/components, as applicable	○ All other necessary payment components or systems, as applicable ○ Any components external to the customer's network—for example, payment processor channels, etc.

ROV Section (PA-DSS) Template	ROV Reporting Details

▪ Description or diagram of each piece of the communication link, including (1) LAN, WAN or Internet, (2) host to host software communication, and (3) within host where software is deployed (for example, how two different processes communicate with each other on the same host)	• Identify all communication points inbound, outbound and between application components, including:
	  ○ LAN, WAN or Internet connections
	  ○ Host to host software communications
	  ○ Communications internal to the host
	  ○ All other connection points applicable to the assessment
	• Provide detailed descriptions and/or diagrams to illustrate each communication point. Ensure descriptions and/or diagrams clearly identify the following:
	  ○ Identification of the communication endpoints (for example, POS terminal, database server, same-host reporting application, etc.)
	  ○ Boundaries between trusted and untrusted components
	  ○ Connection methods and communication protocol
	
	Note: *These detailed descriptions and/or diagrams are additional to the high-level network diagram required above, and should provide a more detailed view of the communication points.*

▪ A dataflow diagram that shows all flows of cardholder data, including authorization, capture, settlement, and chargeback flows as applicable	• Identify all data flows of cardholder data, including:
	  ○ Authorization
	  ○ Capture
	  ○ Settlement
	  ○ Chargeback
	  ○ Any other data flows as applicable
	• For each data flow:
	  ○ Describe how cardholder data is transmitted, processed and/or stored
	  ○ Identify the types of cardholder data involved (for example, full track, PAN, expiry date, etc.)
	  ○ Describe any protection mechanisms (for example, encryption, truncation, masking, etc.) applied to the cardholder data
	  ○ Identify the components involved in the transmission, processing or storage of cardholder data
	
	Note: *Include all types of data flows, including any involving hard copy / paper media.*

ROV Section (PA-DSS) Template	ROV Reporting Details
▪ Brief description of files and tables that store cardholder data, supported by an inventory created (or obtained from the software vendor) and retained by the PA-QSA in the work papers—this inventory should include, for each cardholder data store (file, table, etc.):	• Provide a table that identifies and lists all databases, tables, and files storing cardholder data (including electronic and hard copy) • For each item in the list, provide the following information:
– List of all elements of stored cardholder data	○ All elements of cardholder data stored—for example, PAN, expiry date (include any elements of SAD)
– How data store is secured	○ A description of the security controls in place for protection of the data (for example, encryption, access controls, truncation, etc.)
– How access to data store is logged	○ A description of the logging mechanisms used for logging access to cardholder data (for example, log function built-in to the payment application, sent to operating system logging mechanism, etc.)
▪ List all payment application related software components, including third-party software requirements and dependencies	• Identify and list all payment application ***dependencies***, including software and hardware components, as applicable. Include in the list: ○ Vendor ○ Name of product ○ Version of product ○ Function of product • Identify and list all other ***payment application related software components***, including third-party software requirements. Include in the list: ○ Vendor ○ Name of product ○ Version of product ○ Function of product
▪ Description of payment application's end to end authentication methods, including application authentication mechanism, authentication database, and security of data storage	• Describe the payment application's end to end authentication methods, including details of: ○ The application's authentication mechanism(s), ○ The application's authentication database, and ○ How authentication data (for example, passwords, pins, tokens, etc.) is secured in storage (for example, encryption mechanisms, etc.)

ROV Section (PA-DSS) Template	ROV Reporting Details
▪ Description of role of payment application in a typical implementation and what other types of payment applications are necessary for a full payment implementation	• Describe how the payment application functions in a typical implementation. • Additionally, identify whether any other types of payment applications are necessary for a full payment implementation. If so: – Identify the necessary payment applications – Describe the role of each necessary payment application
▪ Description of the typical customer that this product is sold to (for example, large, small, whether industry-specific, Internet, brick-and-mortar) and vendor's customer's base (for example, market segment, big customer names)	• Identify the vendor's customer's base, including a description of the typical customer this product is sold to, including: ○ Type of customer (for example, merchant, service provider, issuer, etc.) ○ Size of customer (for example, global, national, regional, local, etc.), including country/regions where appropriate ○ Whether the application is designed for industry-specific customers (for example, healthcare, travel, etc.) ○ Customer channel that product is designed for (for example, e-commerce, brick-and-mortar (card present), Mail Order / Telephone Order (MOTO), mixed use, etc.)
▪ Definition of vendor's versioning methodology, to describe/illustrate how vendor indicates major and minor version changes via their version numbers, and to define what types of changes the vendor includes in major and minor version changes	• Describe the vendor's versioning methodology: ○ Describe/illustrate how vendor indicates major and minor version changes via their version numbers. ○ Define what types of changes the vendor includes as: i. Major update ii. Minor update ***Note:*** *Please refer to* the PA-DSS Program Guide *for information on what constitutes a major or minor update*
3. Findings and Observations	
▪ All PA-QSAs must use the following template to provide detailed report descriptions and findings.	• Ensure that the correct ROV template is used for the version of PA-DSS that the assessment was based on. • Ensure that the ROV template defined in the PA-DSS Requirements and Security Assessment Procedures is followed, including: ○ Sections should be presented in the same order as the ROV template. ○ Section numbering should be consistent with the ROV template. ○ Section and table headings should be consistent with the ROV template.
▪ Describe tests performed other than those included in the testing procedures column.	• Identify any tests performed and resultant findings that the assessor feels are relevant to the assessment, but that do not fall under a PA-DSS requirement: ○ Describe any tests performed which are not included in the testing procedures column. ○ List all findings which the assessor feels are relevant which are not included in the findings column.

ROV Section (PA-DSS) Template	ROV Reporting Details
▪ If the assessor determines that a requirement is not applicable for a given payment application, an explanation must be included in the "In Place" column for that requirement.	• If a requirement is deemed to be "in place" due to being N/A, document as such in the "In Place" column, and provide details of how the requirement was verified as being N/A. The details may be recorded in the "Notes" column for the requirement, or in a table format (in an appendix) if there are too many details to fit in the "Notes" column of the requirement. ***Note:*** *The assessor may include a list of the requirements determined to be N/A and a brief justification for each in the "Description of Scope of Review" section. This may be useful if there are a large number of N/A responses, or there is significant impact on how the assessment was performed.*
4. Contact Information and Report Date	
▪ Software vendor contact information (include URL, phone number, and e-mail address)	• Provide the following information for the payment application vendor: ○ Vendor company name ○ Vendor company address ○ Vendor company URL ○ Vendor contact name ○ Vendor contact e-mail address ○ Vendor contact phone number
▪ PA-QSA contact information (include name, phone number and e-mail address)	• Provide the following information for the PA-QSA: ○ PA-QSA company name ○ PA-QSA assessor name ○ PA-QSA contact phone number ○ PA-QSA contact e-mail address
▪ PA-QSA Quality Assurance (QA) primary contact information (include primary QA contact's name, phone number and e-mail address)	• Provide the following information for the PA-QSA Quality Assurance (QA) primary contact: ○ Primary QA contact name ○ Primary QA contact phone number ○ Primary QA contact e-mail address
▪ Date of report	• Provide the date this report was completed

Findings and Observations – PA-DSS Requirements (ROV Section 3) Reporting Methodology

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 1: Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data							
1.1 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 1.1.1 through 1.1.3. ***Notes:*** ▪ *By prohibiting storage of sensitive authentication data after authorization, the assumption is that the transaction has completed the authorization process and the customer has received the final transaction approval. After authorization has completed, this sensitive authentication data cannot be stored.* ▪ *It is permissible for Issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.* ***Aligns with PCI DSS Requirement 3.2***	**1.1.a** If this payment application stores sensitive authentication data, verify that the application is intended only for issuers and/or companies that support issuing services.	• Identify whether the application stores sensitive authentication data after authorization. • If so: i. Confirm that the application is intended for use only by issuers and/or companies that support issuing services. ii. Describe how it was observed that the application is only intended for use by issuers and/or companies that support issuing services. iii. Describe how it was observed that the application stores the data securely.				✓	
	1.1.b For all other payment applications, if sensitive authentication data (see 1.1.1–1.1.3 below) is stored prior to authorization and then deleted, obtain and review methodology for deleting the data to determine that the data is unrecoverable.	For all other payment applications: • Identify whether sensitive authentication data (SAD) is stored prior to authorization and then deleted.				✓	
		• If SAD is *not* stored prior to authorization, describe how the application was tested to confirm that SAD is not stored by the application.				✓	
		• If SAD *is* stored prior to authorization: i. Identify the document that defines the methodology for deleting the data such that that the data is unrecoverable. ii. Describe how the methodology ensures that that the data is unrecoverable.		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	1.1.c For each item of sensitive authentication data below, perform the following steps after completing numerous test transactions that simulate all functions of the payment application, to include generation of error conditions and log entries.	• Describe the test transactions that were performed, and how they simulate all functions of the payment application, including generation of error conditions and log entries.				✓	
1.1.1 After authorization, do not store the full contents of any track from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* ▪ *The accountholder's name,* ▪ *Primary account number (PAN),* ▪ *Expiration date, and* ▪ *Service code* *To minimize risk, store only those data elements needed for business.* ***Aligns with PCI DSS Requirement 3.2.1***	**1.1.1** Use forensic tools and/or methods (commercial tools, scripts, etc.)[1] to examine all output created by the payment application and verify that the full contents of any track from the magnetic stripe on the back of the card or equivalent data on a chip are not stored after authorization. Include at least the following types of files (as well as any other output generated by the payment application): ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Non-volatile memory, including non-volatile cache ▪ Database schemas ▪ Database contents	• Identify the forensic tools and/or methods used to confirm that full track data is not stored after authorization. • Identify the observed data sources, including; i. Incoming transaction data ii. All logs (for example, transaction, history, debugging, error) iii. History files iv. Trace files v. Non-volatile memory, including non-volatile cache vi. Database schemas vii. Database contents viii. All other output generated by the payment application • For each identified data source, describe how it was observed that full track data is not stored after authorization.				✓	

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

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
1.1.2 After authorization, do not store the card-validation value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. ***Aligns with PCI DSS Requirement 3.2.2***	**1.1.2** Use forensic tools and/or methods (commercial tools, scripts, etc.) to examine all output created by the payment application and verify that the three-digit or four-digit card-validation code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization. Include at least the following types of files (as well as any other output generated by the payment application): • Incoming transaction data • All logs (for example, transaction, history, debugging, error) • History files • Trace files • Non-volatile memory, including non-volatile cache • Database schemas • Database contents	• Identify the forensic tools and/or methods used to confirm the three-digit or four-digit card-validation code printed on the card (CVV2, CVC2, CID, CAV2 data) is not stored after authorization. • Identify the observed data sources, including; i. Incoming transaction data ii. All logs (for example, transaction, history, debugging, error) iii. History files iv. Trace files v. Non-volatile memory, including non-volatile cache vi. Database schemas vii. Database contents viii. All other output generated by the payment application • For each identified data source, describe how it was observed that the printed card-validation value or code is not stored after authorization.				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
1.1.3 After authorization, do not store the personal identification number (PIN) or the encrypted PIN block. ***Aligns with PCI DSS Requirement 3.2.3***	**1.1.3** Use forensic tools and/or methods (commercial tools, scripts, etc.) to examine all output created by the payment application, and verify that PINs and encrypted PIN blocks are not stored after authorization. Include at least the following types of files (as well as any other output generated by the payment application). ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Non-volatile memory, including non-volatile cache ▪ Database schemas ▪ Database contents	• Identify the forensic tools and/or methods used confirm PINs and encrypted PIN blocks are not stored after authorization. • Identify the observed data sources, including: i. Incoming transaction data ii. All logs (for example, transaction, history, debugging, error) iii. History files iv. Trace files v. Non-volatile memory, including non-volatile cache vi. Database schemas vii. Database contents viii. Any other output generated by the payment application • For each identified data source, describe how it was observed that PINs and encrypted PIN blocks are not stored after authorization.				✓	
1.1.4 Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the payment application, in accordance with industry-accepted standards for secure deletion, as defined, for example by the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations. ***Note:*** *This requirement applies only if previous versions of the payment application stored sensitive authentication data.* ***Aligns with PCI DSS Requirement 3.2***	**1.1.4.a** Review the *PA-DSS Implementation Guide* prepared by the vendor and verify the documentation includes the following instructions for customers and resellers/integrators: ▪ That historical data must be removed (magnetic stripe data, card validation codes, PINs, or PIN blocks stored by previous versions of the payment application) ▪ How to remove historical data ▪ That such removal is absolutely necessary for PCI DSS compliance	• Identify whether any previous version of the payment application stored: i. Magnetic stripe data ii. Card validation values or codes iii. PINs or PIN block data • If so, briefly describe how the *PA-DSS Implementation Guide* includes the following instructions for customers and resellers/integrators: i. That historical data must be removed (magnetic stripe data, card validation codes, PINs, or PIN blocks stored by previous versions of the payment application) ii. Detailed procedures for removing historical data iii. That such removal is absolutely necessary for PCI DSS compliance • Describe how the process provided in the *Implementation Guide* for removing historical data was observed to be effective.		✓		✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	1.1.4.b Verify the vendor provides a secure wipe tool or procedure to remove the data.	• If any previous version of the payment application stored magnetic stripe data, card validation values or codes, PINs, or PIN block data: i. Identify the secure wipe tool or procedure the vendor provides to remove the data.				✓	
	1.1.4.c Verify, through the use of forensic tools and/or methods, that the secure wipe tool or procedure provided by vendor securely removes the data, in accordance with industry-accepted standards for secure deletion of data.	• If any previous version of the payment application stored magnetic stripe data, card validation values or codes, PINs, or PIN block data: i. Identify the forensic tools and/or methods used to confirm the tool or procedure securely removes the data. ii. Identify the industry-accepted standard(s) for secure deletion of data. iii. Describe how the tool or procedure was observed to securely remove the data in accordance with the industry-accepted standards.				✓	
1.1.5 Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other data sources received from customers, to ensure that magnetic stripe data, card validation codes or values, and PINs or PIN block data are not stored on software vendor systems. These data sources must be collected in limited amounts and only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use. ***Aligns with PCI DSS Requirement 3.2***	**1.1.5.a** Examine the software vendor's procedures for troubleshooting customers' problems and verify the procedures include: ▪ Collection of sensitive authentication data only when needed to solve a specific problem ▪ Storage of such data in a specific, known location with limited access ▪ Collection of only a limited amount of data needed to solve a specific problem ▪ Encryption of sensitive authentication data while stored ▪ Secure deletion of such data immediately after use	• Identify the document that contains the software vendor's procedures for troubleshooting customers' problems. • Briefly describe how the documented procedures ensure: i. Collection of sensitive authentication data only when needed to solve a specific problem ii. Storage of such data in a specific, known location with limited access iii. Collection of only a limited amount of data needed to solve a specific problem iv. Encryption of sensitive authentication data while stored v. Secure deletion of such data immediately after use		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	1.1.5.b Select a sample of recent troubleshooting requests from customers, and verify each event followed the procedure examined at 1.1.5.a.	• Identify the sample of customer troubleshooting requests observed. • For each troubleshooting request in the sample, describe how the documented procedures were observed to be followed, including: i. Collection of sensitive authentication data only when needed to solve a specific problem ii. Storage of such data in a specific, known location with limited access iii. Collection of only a limited amount of data needed to solve a specific problem iv. Encryption of sensitive authentication data while stored v. Secure deletion of such data immediately after use				✓	✓
	1.1.5.c Review the *PA-DSS Implementation Guide* prepared by the vendor and verify the documentation includes the following instructions for customers and resellers/integrators: ▪ Collect sensitive authentication only when needed to solve a specific problem. ▪ Store such data only in specific, known locations with limited access. ▪ Collect only the limited amount of data needed to solve a specific problem. ▪ Encrypt sensitive authentication data while stored. ▪ Securely delete such data immediately after use.	• Briefly describe how the *PA-DSS Implementation Guide* provides the following instructions for customers and resellers/integrators: i. Collect sensitive authentication only when needed to solve a specific problem ii. Store such data only in specific, known locations with limited access iii. Collect only the limited amount of data needed to solve a specific problem iv. Encrypt sensitive authentication data while stored v. Securely delete such data immediately after use		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 2: Protect stored cardholder data							
2.1 Software vendor must provide guidance to customers regarding purging of cardholder data after expiration of customer-defined retention period. ***Aligns with PCI DSS Requirement 3.1***	**2.1** Review the *PA-DSS Implementation Guide* prepared by the vendor and verify the documentation includes the following guidance for customers and resellers/integrators: ▪ That cardholder data exceeding the customer-defined retention period must be purged ▪ A list of all locations where the payment application stores cardholder data (so that customer knows the locations of data that needs to be deleted) ▪ Instructions for configuring the underlying software or systems (such as OS, databases, etc.) to prevent inadvertent capture or retention of cardholder data. For example, system backup or restore points.	• Briefly describe how the *PA-DSS Implementation Guide* includes the following details for customers and resellers/integrators: i. Guidance that cardholder data exceeding the customer-defined retention period must be purged ii. A detailed list of all locations where the payment application stores cardholder data (so that customer knows the locations of data that needs to be deleted) iii. Detailed instructions for configuring the underlying software or systems (such as OS, databases, etc.) to prevent inadvertent capture or retention of cardholder data—for example, system backup or restore points • Describe how all locations where the payment application stores cardholder data were observed to confirm that the list provided in the *Implementation Guide* is complete. • Describe how the instructions provided in the *Implementation Guide* for configuring underlying software or systems to prevent inadvertent capture or retention of cardholder data were observed to be effective.		✓		✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
2.2 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). ***Notes:*** ▪ *This requirement does not apply to those employees and other parties with a legitimate business need to see full PAN;* ▪ *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.* ***Aligns with PCI DSS Requirement 3.3***	**2.2** Review displays of credit card data, including but not limited to POS devices, screens, logs, and receipts, to determine that credit card numbers are masked when displaying cardholder data, except for those with a legitimate business need to see full credit card numbers.	• Identify all instances where credit card data is displayed by the application (including but not limited to POS devices, screens, logs, and receipts). • For each instance where credit card data is displayed: i. Identify whether PAN is masked for each display. ii. Describe how observed PAN displays were masked. iii. Describe how the payment application limits displays of full PAN to those with a legitimate business need to see full PAN.				✓	
2.3 Render PAN unreadable anywhere it is stored, (including data on portable digital media, backup media, and in logs) by using any of the following approaches: ▪ One-way hashes based on strong cryptography (hash must be of the entire PAN) ▪ Truncation (hashing cannot be used to replace the truncated segment of PAN) ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key management processes and procedures.	**2.3** Verify that the PAN is rendered unreadable anywhere it is stored, as follows.						
	2.3.a Examine the method used to protect the PAN, including the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using any of the following methods: • One-way hashes based on strong cryptography. • Truncation • Index tokens and pads, with the pads being securely stored • Strong cryptography, with associated key-management processes and procedures	• Identify the method used to protect PAN. • Identify the encryption algorithms used (if applicable). • Describe how the method was observed to render PAN unreadable using any of the following methods: ○ One-way hashes based on strong cryptography ○ Truncation ○ Index tokens and pads, with the pads being securely stored ○ Strong cryptography, with associated key-management processes and procedures				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Notes: ▪ *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are generated by a payment application, additional controls should be in place to ensure that hashed and truncated versions cannot be correlated to reconstruct the original PAN.* ▪ *The PAN must be rendered unreadable anywhere it is stored, even outside the payment application.* ***Aligns with PCI DSS Requirement 3.4***	**2.3.b** Examine several tables or files from data repositories created or generated by the application to verify the PAN is rendered unreadable.	• Identify all data repositories created or generated by the application. • For each identified data repository: i. Identify the tables or files created or generated by the application that were examined. ii. Describe how the observed tables or files confirm that PAN is rendered unreadable				✓	
	2.3.c If the application creates or generates files for use outside the application (for example, files generated for export or backup), including for storage on removable media, examine a sample of generated files, including those generated on removable media (for example, back-up tapes), to confirm that the PAN is rendered unreadable.	• Identify all instances where the application creates or generates files for use outside the application (for example, files generated for export or backup), including for storage on removable media. • For each identified instance: i. Identify the sample of generated files observed. ii. Describe how the observed files confirm that PAN is rendered unreadable.				✓	✓
	2.3.d Examine a sample of audit logs created or generated by the application to confirm that the PAN is rendered unreadable or removed from the logs.	• Identify the sample of audit logs observed. • Describe how the observed logs confirm that PAN is rendered unreadable or removed from the logs.				✓	✓

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	2.3.e If the software vendor stores the PAN for any reason (for example, because log files, debugging files, and other data sources are received from customers for debugging or troubleshooting purposes), verify that the PAN is rendered unreadable in accordance with Requirements 2.3.a through 2.3.d, above.	• Identify all instances where the software vendor stores PAN for any reason (for example, log files, debugging files, and other data sources received from customers for debugging or troubleshooting purposes). • For each identified instance: i. Identify the locations where the PAN is stored ii. Describe how the following was observed: ○ PAN was observed to be rendered unreadable using any of the methods defined in PA-DSS Requirement 2.3.a. ○ PAN was observed to be rendered unreadable in several tables or files from data repositories, per PA-DSS Requirement 2.3.b. ○ PAN was observed to be rendered unreadable in files generated for export or backup, including for storage on removable media, per PA-DSS Requirement 2.3.c. ○ PAN was observed to be rendered unreadable or removed from audit logs, per PA-DSS Requirement 2.3.d.				✓	
2.4 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts. ***Aligns with PCI DSS Requirement 3.4.2***	**2.4** If disk encryption is used, verify that it is implemented as follows:						
	2.4.a Verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases).	• Identify whether disk encryption is used • If disk encryption is used: i. Describe the mechanism for managing logical access independently of native operating system access control mechanisms. ii. Describe how the mechanism was observed to manage logical access separately from native operating system access control mechanisms. iii. Describe how decryption keys were observed not to be tied to user accounts.				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	2.4.b Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).	• If disk encryption is used, describe how cryptographic keys were observed to be stored securely.				✓	
	2.4.c If the application creates or generates files on removable media, verify that cardholder data on removable media is encrypted wherever stored.	• If disk encryption is used, identify whether the application creates or generates files on removable media. • For each instance where files are created or generated on removable media, describe how cardholder data was observed to be encrypted wherever stored.				✓	
2.5 Payment application must protect any keys used to secure cardholder data against disclosure and misuse. ***Note:*** *This requirement also applies to key-encryption keys used to protect data-encrypting keys—such key-encryption keys must be at least as strong as the data-encrypting key.* ***Aligns with PCI DSS Requirement 3.5***	**2.5** Verify the payment application protects any keys used to secure cardholder data against disclosure and misuse, as follows:						
	2.5.a Examine methodology used by application to protect keys, to verify that controls are in place that restrict access to keys.	• Describe the methodology(s) used by the application to protect keys against disclosure and misuse. • Describe how access to keys was observed to be restricted.				✓	
	2.5.b Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys	• Identify the system configuration files observed. • Describe how keys were observed to be stored in encrypted format. • Describe how key-encrypting keys were observed to be stored separately from data-encrypting keys.	✓			✓	
	2.5.c Review the *PA-DSS Implementation Guide* prepared by the vendor and verify that customers and resellers/integrators are strongly advised to: ▪ Restrict access to keys to the fewest number of custodians necessary. ▪ Store keys securely in the fewest possible locations and forms.	• Briefly describe how the *PA-DSS Implementation Guide* strongly advises customers and resellers/integrators to: i. Restrict access to keys to the fewest number of custodians necessary. ii. Store keys securely in the fewest possible locations and forms.		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
2.6 Payment application must implement key management processes and procedures for cryptographic keys used for encryption of cardholder data, including at least the following: ***Aligns with PCI DSS Requirement 3.6***	**2.6.a** Review the *PA-DSS Implementation Guide* prepared by the vendor and verify the documentation includes the following instructions for customers and resellers/integrators: ▪ How to securely generate, distribute, protect, change, store, and retire/replace encryption keys, where customers or resellers/integrators are involved in these key management activities ▪ A sample Key Custodian form for key custodians to acknowledge that they understand and accept their key-custodian responsibilities ▪ How to perform key management functions defined in 2.6.1 through 2.6.7 below, as required for PCI DSS compliance	• Briefly describe how the *PA-DSS Implementation Guide* includes the following: i. Instructions for customers and resellers/integrators on how to perform the following, where customers or resellers/integrators are involved in these key-management activities: ○ Securely generate encryption keys ○ Securely distribute encryption keys ○ Securely protect encryption keys ○ Securely change encryption keys ○ Securely store encryption keys ○ Securely retire/replace encryption keys ii. A sample Key Custodian form for key custodians to acknowledge that they understand and accept their key-custodian responsibilities. iii. Instructions on how to perform the following key management functions as required for PCI DSS compliance: ○ Generation of strong cryptographic keys ○ Secure cryptographic key distribution ○ Secure cryptographic key storage ○ Cryptographic key changes for keys that have reached the end of their cryptoperiod ○ Retirement or replacement of keys, as follows: ▪ When the integrity of the key has been weakened ▪ When keys are suspected of being compromised ▪ Any retained keys are securely archived and are not used for encryption operations ○ Use of split knowledge and dual control of keys wherever manual clear-text key-management operations are used ○ Prevention of unauthorized substitution of cryptographic keys		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	2.6.b Verify the payment application implements key-management techniques for keys, as follows:						
2.6.1 Generation of strong cryptographic keys	**2.6.1** Verify that key-management procedures are implemented to generate strong keys.	• Describe how the payment application was observed to implement procedures to generate strong keys.				✓	
2.6.2 Secure cryptographic key distribution	**2.6.2** Verify that key-management procedures are implemented to securely distribute keys.	• Describe how the payment application was observed to implement procedures to securely distribute keys.				✓	
2.6.3 Secure cryptographic key storage	**2.6.3** Verify that key-management procedures are implemented to securely store keys.	• Describe how the payment application was observed to implement procedures to securely store keys.				✓	
2.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57.	**2.6.4** Verify that key-management procedures are implemented to enforce key changes at the end of the defined cryptoperiod.	• Describe how the payment application was observed to implement procedures to enforce key changes at the end of the defined cryptoperiod.				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
2.6.5 Retirement or replacement of keys (for example: by archiving, destruction, and/or revocation as applicable) as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key, etc.) or keys are suspected of being compromised. ***Note:*** *If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should be used only for decryption/verification purposes.*	**2.6.5.a** Verify that key-management procedures are implemented to retire keys when the integrity of the key has been weakened.	• Describe how the payment application was observed to implement procedures to retire keys when the integrity of the key has been weakened.				✓	
	2.6.5.b Verify that key-management procedures are implemented to replace known or suspected compromised keys.	• Describe how the payment application was observed to implement procedures to replace known or suspected compromised keys.				✓	
	2.6.5.c If retired or replaced cryptographic keys are retained, verify that the application does not use these keys for encryption operations.	• Identify whether retired or replaced cryptographic keys are retained. • If so, describe how it was observed that the payment application does not use these keys for encryption operations.				✓	
2.6.6 If the payment application supports manual clear-text cryptographic key management operations, these operations must enforce split knowledge and dual control (for example, requiring two or three people, each knowing only their own part of the key, to reconstruct the whole key). ***Note:*** *Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	**2.6.6** Verify that manual clear-text key-management procedures require split knowledge and dual control of keys.	• Identify whether the payment application supports manual clear-text cryptographic key management operations. • If so, describe how the payment application was observed to enforce split knowledge and dual control of keys for all manual clear-text key-management operations.				✓	
2.6.7 Prevention of unauthorized substitution of cryptographic keys	**2.6.7** Verify that key-management procedures are implemented to prevent unauthorized substitution of keys.	• Describe how the payment application was observed to implement procedures to prevent unauthorized substitution of keys.				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
2.7 Render irretrievable any cryptographic key material or cryptogram stored by previous versions of the payment application, in accordance with industry-accepted standards. These are cryptographic keys used to encrypt or verify cardholder data. ***Notes:*** ▪ *Cryptographic key materials and/or cryptograms may be rendered irretrievable through the use of tools or processes including but not limited to:* ○ *Secure deletion, as defined, for example, in the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations.* ○ *The deletion of the key-encryption key (KEK) provided that residual data-encryption keys only exist in encrypted form under the deleted KEK.* ▪ *This requirement applies only if previous versions of the payment application used cryptographic key materials or cryptograms to encrypt cardholder data.* ***Aligns with PCI DSS Requirement 3.6***	**2.7.a** Review the *PA-DSS Implementation Guide* prepared by the vendor and verify the documentation includes the following instructions for customers and resellers/integrators: • That cryptographic material must be rendered irretrievable • How to render cryptographic material irretrievable • That such irretrievability is absolutely necessary for PCI DSS compliance • How to re-encrypt historic data with new keys	• Briefly describe how the *PA-DSS Implementation Guide* includes the following instructions for customers and resellers/integrators: i. That cryptographic material must be rendered irretrievable ii. How to render cryptographic material irretrievable iii. That such irretrievability is absolutely necessary for PCI DSS compliance iv. How to re-encrypt historic data with new keys		✓			
	2.7.b Verify vendor provides a tool or procedure to render cryptographic material irretrievable.	• Describe the tool or procedure provided by the vendor for rendering cryptographic material irretrievable.				✓	
	2.7.c Verify, through use of forensic tools and/or methods, that the secure wipe tool or procedure renders the cryptographic material irretrievable, in accordance with industry-accepted standards.	• Identify the forensic tools and/or methods used to confirm that the secure wipe tool or procedure renders the cryptographic material irretrievable. • Describe how the vendor-provided tool or procedure was observed to render the cryptographic material irretrievable. • Identify the industry-accepted standards.				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 3: Provide secure authentication features							
3.1 The payment application must support and enforce the use of unique user IDs and secure authentication for all administrative access and for all access to cardholder data. Secure authentication must be enforced to all accounts, generated or managed by the application, by the completion of installation and for subsequent changes after installation. The application must require the following: ***Note:*** *These password controls are not intended to apply to personnel who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by personnel with administrative capabilities, for access to systems with cardholder data, and for access controlled by the payment application.* *This requirement applies to the payment application and all associated tools used to view or access cardholder data.* ***Aligns with PCI DSS Requirements 8.1, 8.2, and 8.5.8–8.5.15***	**3.1.a** Examine *PA-DSS Implementation Guide* created by vendor to verify the following: ▪ Customers and resellers/integrators are advised that the payment application enforces secure authentication for all authentication credentials that the application generates by: ○ Enforcing secure changes to authentication credentials by the completion of installation (See below at 3.1.1 through 3.1.10). ○ Enforcing secure changes for any subsequent changes (after installation) to authentication credentials (See below at 3.1.1 through 3.1.10) ▪ Customers and resellers/integrators are advised to assign secure authentication to any default accounts (even if they won't be used), and then disable or do not use the accounts. ▪ When authentication credentials are used by the payment application (but are not generated or managed by the application), customers and resellers/integrators are provided clear and unambiguous directions on how, by the completion of installation and for any changes after installation, to change authentication credentials and create strong authentication per Requirements 3.1.1 through 3.1.10 below, for all application level accounts with administrative access and for all access to cardholder data.	• Briefly describe how the *PA-DSS Implementation Guide* includes the following advice to customers and resellers/integrators: i. The payment application enforces secure authentication for all authentication credentials that the application generates by: ○ Enforcing secure changes to authentication credentials by the completion of installation in accordance with PA-DSS Requirements 3.1.1 - 3.1.10 ○ Enforcing secure changes for any subsequent changes (after installation) to authentication credentials in accordance with PA-DSS Requirements 3.1.1 - 3.1.10 ii. Secure authentication should be assigned to any default accounts (even if they won't be used). iii. Default accounts that won't be used should be disabled or not used. • Identify any authentication credentials used by the payment application but that are not generated or managed by the application. • For all authentication credentials used by the payment application (but not generated or managed by the application), briefly describe how the *PA-DSS Implementation Guide* provides clear and unambiguous directions on how to change authentication credentials and create strong authentication per Requirements 3.1.1 through 3.1.10: i. For all application level accounts with administrative access: ○ By the completion of installation ○ For any changes after installation ii. For all access to cardholder data: ○ By the completion of installation ○ For any changes after installation		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	3.1.b Test the payment application to verify the payment application does not use (or require the use of) default administrative accounts for other necessary software (for example, the payment application must not use the database default administrative account).	• Describe how the payment application was tested for the use of default administrative accounts for other necessary software. • Describe how it was observed that the payment application: i. Does not use default administrative accounts for other necessary software ii. Requires the use of default administrative accounts for other necessary software				✓	
	3.1.c If the payment application generates or manages authentication credentials, test the application to verify that it enforces changes to any default payment application passwords by the completion of the installation process.	• Identify whether the application generates or manages authentication credentials. • If so, describe how the payment application was observed to enforce changes to any default payment application passwords by the completion of the installation process.				✓	
	3.1.d For accounts that are generated or managed by the application, test the application to verify that it enforces unique user IDs and secure authentication according to 3.1.1 through 3.1.10 below, for all administrative access and for all access to cardholder data. Ensure that secure authentication requirements are enforced: ○ By the completion of the installation process, and ○ For subsequent changes after installation. (Examples of subsequent changes include but are not limited to any changes that result in user accounts reverting to default settings, any changes to existing account settings, and changes that generate new accounts or recreate existing accounts.)						

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
3.1.1 The payment application assigns unique IDs for user accounts. ***Aligns with PCI DSS Requirements 8.1***	**3.1.1** Confirm that the payment application assigns unique user IDs:						
	3.1.1.a By completion of the installation process	• Describe how the payment application was observed to assign unique user IDs by completion of the installation process.				✓	
	3.1.1.b For subsequent changes after installation	• For subsequent changes after installation, describe how the payment application was observed to assign unique user IDs.				✓	
3.1.2 The payment application employs at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric ***Aligns with PCI DSS Requirements 8.2***	**3.1.2** Confirm that the payment application requires at least one of the defined authentication methods:						
	3.1.2.a By completion of the installation process	• Describe how the payment application was observed to require at least one of the defined authentication methods by completion of the installation process. • Identify the authentication method(s) observed to be required				✓	
	3.1.2.b For subsequent changes after installation	• For subsequent changes after installation, describe how the payment application was observed to require at least one of the defined authentication methods for subsequent changes after installation. • Identify the authentication method(s) observed to be required.				✓	
3.1.3 The payment application does **not** require or use any group, shared, or generic accounts and passwords. ***Aligns with PCI DSS Requirement 8.5.8***	**3.1.3** Confirm that the payment application does not rely on or use any group, shared, or generic accounts and passwords:						
	3.1.3.a By completion of the installation process	• Describe how the payment application was observed to not rely on or use any of the following by completion of the installation process: i. Group accounts and passwords ii. Shared accounts and passwords iii. Generic accounts and passwords				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	3.1.3.b For subsequent changes after installation.	• For subsequent changes after installation, describe how the payment application was observed to not rely on or use any of the following: i. Group accounts and passwords ii. Shared accounts and passwords iii. Generic accounts and passwords				✓	
3.1.4 The payment application requires changes to user passwords at least every 90 days. ***Aligns with PCI DSS Requirement 8.5.9***	**3.1.4** Confirm that the payment application requires users to change passwords at least every 90 days:						
	3.1.4.a By completion of the installation process	• Describe how the payment application was observed to require users to change passwords at least every 90 days by completion of the installation process.				✓	
	3.1.4.b For subsequent changes after installation	• For subsequent changes after installation, describe how the payment application was observed to require users to change passwords at least every 90 days.				✓	
3.1.5 The payment application requires a minimum password length of at least seven characters. ***Aligns with PCI DSS Requirement 8.5.10***	**3.1.5** Confirm that the payment requires passwords to be at least seven characters long:						
	3.1.5.a By completion of the installation process	• Describe how the payment application was observed to require passwords to be at least seven characters long by completion of the installation process.				✓	
	3.1.5.b For subsequent changes after installation	• For subsequent changes after installation, describe how the payment application was observed to require passwords to be at least seven characters long.				✓	
3.1.6 The payment application requires that passwords contain both numeric and alphabetic characters. ***Aligns with PCI DSS Requirement 8.5.11***	**3.1.6** Confirm that the payment application requires passwords to contain both numeric and alphabetic characters.						

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	3.1.6.a By completion of the installation process	• Describe how the payment application was observed to require passwords to contain the following by completion of the installation process: i. Numeric characters ii. Alphabetic characters				✓	
	3.1.6.b For subsequent changes after installation	• For subsequent changes after installation, describe how the payment application was observed to require passwords to contain the following: i. Numeric characters ii. Alphabetic characters				✓	
3.1.7 The payment application keeps password history and requires that a new password is different than any of the last four passwords used. ***Aligns with PCI DSS Requirement 8.5.12***	**3.1.7** Confirm that the payment application keeps password history and requires that a new password is different than any of the last four passwords used:						
	3.1.7.a By completion of the installation process	• Describe how the payment application was observed to perform the following by the completion of the installation process: i. Keep password history ii. Require that a new password is different than any of the last four passwords used				✓	
	3.1.7.b For subsequent changes after installation	• For subsequent changes after installation, describe how the payment application was observed to perform the following: i. Keep password history ii. Require that a new password is different than any of the last four passwords used				✓	
3.1.8 The payment application limits repeated access attempts by locking out the user account after not more than six logon attempts. ***Aligns with PCI DSS Requirement 8.5.13***	**3.1.8** Confirm that the payment locks out user account after not more than six invalid logon attempts.						
	3.1.8.a By completion of the installation process	• Describe how the payment application was observed to lock out user accounts after not more than six invalid logon attempts, by the completion of the installation process.				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	3.1.8.b For subsequent changes after installation	• For subsequent changes after installation, describe how the payment application was observed to lock out user accounts after not more than six invalid logon attempts.				✓	
3.1.9 The payment application sets the lockout duration to a minimum of 30 minutes or until administrator enables the user ID. ***Aligns with PCI DSS Requirement 8.5.14***	**3.1.9** Confirm that the payment application locks out user accounts for a minimum of 30 minutes or until a system administrator resets the account.						
	3.1.9.a By completion of the installation process	• Describe how the payment application was observed to lock out user accounts for a minimum of 30 minutes or until a system administrator resets the account, by the completion of the installation process.				✓	
	3.1.9.b For subsequent changes after installation	• For subsequent changes after installation, describe how the payment application was observed to lock out user accounts for a minimum of 30 minutes or until a system administrator resets the account.				✓	
3.1.10 If a payment application session has been idle for more than 15 minutes, the application requires the user to re-authenticate to re-activate the session. ***Aligns with PCI DSS Requirement 8.5.15***	**3.1.10** Confirm that the payment sets a session idle time out to 15 minutes or less.						
	3.1.10.a By completion of the installation process	• Describe how the payment application was observed to set a session idle time out to 15 minutes or less by the completion of the installation process.				✓	
	3.1.10.b For subsequent changes after installation	• For subsequent changes after installation, describe how the payment application was observed to set a session idle time out to 15 minutes or less.				✓	
3.2 Software vendor must provide guidance to customers that all access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication. ***Aligns with PCI DSS Requirements 8.1 and 8.2***	**3.2** Examine *PA-DSS Implementation Guide* created by vendor to verify customers and resellers/integrators are strongly advised to control access, via unique user ID and PCI DSS-compliant secure authentication, to any PCs, servers, and databases with payment applications and cardholder data.	• Briefly describe how the *PA-DSS Implementation Guide* strongly advises customers and resellers/integrators to: i. Control access to any PCs, servers, and databases with payment applications via unique user ID and PCI DSS-compliant secure authentication ii. Control access to any PCs, servers, and databases with cardholder data via unique user ID and PCI DSS-compliant secure authentication		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
3.3 Render payment application passwords unreadable during transmission and storage, using strong cryptography based on approved standards. ***Aligns with PCI DSS Requirement 8.4***	**3.3** Examine payment application password files during storage and transmission to verify that strong cryptography is used to render passwords unreadable at all times.	• Identify password files observed (in storage and transmission). • Identify the strong cryptography used to render passwords unreadable during: i. Storage ii. Transmission • Describe how observation of password files verifies that strong cryptography is used to render passwords unreadable at all times during: i. Storage ii. Transmission	✓			✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 4: Log payment application activity							
4.1 At the completion of the installation process, the "out of the box" default installation of the payment application must log all user access (especially users with administrative privileges), and be able to link all activities to individual users. ***Aligns with PCI DSS Requirement 10.1***	**4.1.a** Examine payment application settings to verify that payment application audit trails are automatically enabled or are available to be enabled by customers.	• Identify whether payment application audit trails are automatically enabled or are available to be enabled by customers. • Describe how observed payment application settings ensure that payment application audit trails are automatically enabled or are available to be enabled by customers.	✓			✓	
	4.1.b If payment application log settings are configurable by the customer and resellers/integrators, or customers or resellers/integrators are responsible for implementing logging, examine *PA-DSS Implementation Guide* prepared by the vendor to verify the following information is included: • How to set PCI DSS-compliant log settings, per PA-DSS Requirements 4.2, 4.3 and 4.4 below. • That logs should not be disabled and doing so will result in non-compliance with PCI DSS.	• Identify whether payment application log settings are configurable by the customer and resellers/integrators.	✓				
		• Identify whether customers and resellers/integrators are responsible for implementing logging.				✓	
		• If log settings are configurable by the customer or reseller/integrator, or the customer or reseller/integrator are responsible for implementing logging, briefly describe how the *PA-DSS Implementation Guide* includes the following instructions: i. How to set PCI DSS-compliant log settings, as follows: ○ To reconstruct the events defined in PA-DSS Requirements 4.2.1 – 4.2.7 ○ To record at least the audit trail entries identified in PA-DSS Requirements 4.3.1 – 4.3.6, for each audited event ○ To facilitate centralized logging as defined in PA-DSS Requirement 4.4 ii. That logs should not be disabled and doing so will result in non-compliance with PCI DSS.		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
4.2 Payment application must provide an audit trail to reconstruct the following events: ***Aligns with PCI DSS Requirement 10.2***	**4.2** Test the payment application and examine payment application audit logs and audit log settings, and perform the following:						
4.2.1 All individual accesses to cardholder data from the application	**4.2.1** Verify all individual access to cardholder data through the payment application is logged.	• Describe how the payment application was tested to confirm that all individual access from the application to cardholder data is logged. • Describe the application audit log settings observed to log all individual access from the application to cardholder data. • Describe how the observed audit logs include all individual access from the application to cardholder data.	✓			✓	
4.2.2 All actions taken by any individual with administrative privileges as assigned in the application	**4.2.2** Verify actions taken by any individual with administrative privileges to the payment application are logged.	• Describe how the payment application was tested to confirm that all actions taken by any individual with root or administrative privileges are logged. • Describe the application audit log settings observed to log all actions taken by any individual with root or administrative privileges. • Describe how the observed audit logs include all actions taken by any individual with root or administrative privileges.	✓			✓	
4.2.3 Access to application audit trails managed by or within the application	**4.2.3** Verify access to application audit trails managed by or within the application is logged.	• Describe how the payment application was tested to confirm that access to application audit trails managed by or within the application is logged. • Describe the application audit log settings observed to log access to application audit trails managed by or within the application. • Describe how the observed audit logs include access to all application audit trails managed by or within the application.	✓			✓	
4.2.4 Invalid logical access attempts	**4.2.4** Verify invalid logical access attempts are logged.	• Describe how the payment application was tested to confirm that invalid logical access attempts are logged. • Describe the application audit log settings observed to log invalid logical access attempts. • Describe how the observed audit logs include invalid logical access attempts.	✓			✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
4.2.5 Use of the application's identification and authentication mechanisms	**4.2.5** Verify use of the payment application's identification and authentication mechanisms is logged.	• Describe how the payment application was tested to confirm the following is logged: i. Use of the payment application's identification mechanisms ii. Use of the payment application's authentication mechanisms • Describe the application audit log settings observed to log: i. Use of the payment application's identification mechanisms ii. Use of the payment application's authentication mechanisms • Describe how the observed audit logs include: i. Use of the payment application's identification mechanisms ii. Use of the payment application's authentication mechanisms	✓			✓	
4.2.6 Initialization of the application audit logs	**4.2.6** Verify initialization of application audit logs is logged.	• Describe how the payment application was tested to confirm that initialization of application audit logs is logged. • Describe the audit log settings observed to log initialization of application audit logs. • Describe how the observed audit logs include initialization of application audit logs.	✓			✓	
4.2.7 Creation and deletion of system-level objects within or by the application	**4.2.7** Verify the creation and deletion of system-level objects within or by the application is logged.	• Describe how the payment application was tested to confirm the following is logged: i. Creation of system-level objects within or by the application ii. Deletion of system-level objects within or by the application • Describe the audit log settings observed to log: i. Creation of system-level objects within or by the application ii. Deletion of system-level objects within or by the application • Describe how the observed audit logs include: i. Creation of system level objects within or by the application ii. Deletion of system level objects within or by the application	✓			✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
4.3 Payment application must record at least the following audit trail entries for each event: ***Aligns with PCI DSS Requirement 10.3***	**4.3** Test the payment application and examine the payment application's audit logs and audit log settings, and, for each auditable event (from 4.2), perform the following:						
4.3.1 User identification	**4.3.1** Verify user identification is included in log entries.	• Describe how the payment application was tested to confirm that user identification is recorded in log entries. • Describe the audit log settings observed to record user identification. • *For each auditable event from 4.2.1 – 4.2.7*: i. Describe how user identification was observed to be included in all audit log entries.	✓			✓	
4.3.2 Type of event	**4.3.2** Verify type of event is included in log entries.	• Describe how the payment application was tested to confirm that type of event is recorded in log entries. • Describe the audit log settings observed to record the type of event. • *For each auditable event from 4.2.1 – 4.2.7*: i. Describe how type of event was observed to be included in all audit log entries.	✓			✓	
4.3.3 Date and time	**4.3.3** Verify date and time stamp is included in log entries.	• Describe how the payment application was tested to confirm that date and time is recorded in log entries. • Describe the audit log settings observed to record the date and time. • *For each auditable event from 4.2.1 – 4.2.7*: i. Describe how date and time was observed to be included in all audit log entries.	✓			✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
4.3.4 Success or failure indication	**4.3.4** Verify success or failure indication is included in log entries.	• Describe how the payment application was tested to confirm that success or failure indication is recorded in log entries. • Describe the audit log settings observed to record the success or failure indication. • *For each auditable event from 4.2.1 – 4.2.7:* i. Describe how success or failure indication was observed to be included in all audit log entries.	✓			✓	
4.3.5 Origination of event	**4.3.5** Verify origination of event is included in log entries.	• Describe how the payment application was tested to confirm that origination of the event is recorded in log entries. • Describe the audit log settings observed to record the origination of the event. • *For each auditable event from 4.2.1 – 4.2.7:* i. Describe how origination of the event was observed to be included in all audit log entries.	✓			✓	
4.3.6 Identity or name of affected data, system component, or resource	**4.3.6** Verify identity or name of affected data, system component, or resources is included in log entries.	• Describe how the payment application was tested to confirm that the identity or name of affected data, system component, or resource is recorded in log entries. • Describe the audit log settings observed to record the identity or name of affected data, system component, or resource. • *For each auditable event from 4.2.1 – 4.2.7:* i. Describe how the identity or name of affected data, system component, or resource was observed to be included in all audit log entries.	✓			✓	
4.4. Payment application must facilitate centralized logging. ***Note:*** *Examples of this functionality may include, but are not limited to:*	**4.4.a** Validate that payment application provides functionality that facilitates a merchant's ability to assimilate logs into their centralized log server.	• Describe the functionality provided by the payment application to facilitate a merchant's ability to assimilate logs into their centralized log server. • Describe how the functionality was observed to facilitate centralized logging.				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
▪ Logging via industry standard log file mechanisms such as Common Log File System (CLFS), Syslog, delimited text, etc. ▪ Providing functionality and documentation to convert the application's proprietary log format into industry standard log formats suitable for prompt, centralized logging. ***Aligns with PCI DSS Requirement 10.5.3***	**4.4.b** Examine the *PA-DSS Implementation Guide* prepared by the vendor to verify that customers and resellers/integrators are provided with instructions and procedures for incorporating the payment application logs into a centralized logging environment.	• Briefly describe how the *PA-DSS Implementation Guide* provides instructions and procedures for customers and resellers/integrators for incorporating the payment application logs into a centralized logging environment.		✓			
Requirement 5: Develop secure payment applications							
5.1 The software vendor develops payment applications in accordance with PCI DSS and PA-DSS (for example, secure authentication and logging) and based on industry best practices, and incorporates information security throughout the software development life cycle. These processes must include the following: ***Aligns with PCI DSS Requirement 6.3***	**5.1.a** Obtain and examine written software development processes to verify that processes are based on industry standards and/or best practices.	• Identify the document which defines vendor software development processes based on industry standards and/or best practice. • Identify the industry standards and/or best practices used.		✓			
	5.1.b Verify that information security is included throughout the software development life cycle.	• Describe how the documented software development processes include information security throughout the software development life cycle. • Describe how the observed software development processes confirm that information security is included throughout the software development life cycle.		✓		✓	
	5.1.c Verify that software applications are developed in accordance with PCI DSS and PA-DSS Requirements.	• Describe how the documented software development processes require that software applications are developed in accordance with: i. PCI DSS Requirements ii. PA-DSS Requirements • Describe how the observed software development processes confirm that software applications are developed in accordance with: i. PCI DSS Requirements ii. PA-DSS Requirements		✓		✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	5.1.d From an examination of written software development processes, interviews of software developers, and examination of the final payment application product, verify that:						
5.1.1 Live PANs are not used for testing or development. ***Aligns with PCI DSS Requirement 6.4.3***	**5.1.1** Live PANs are not used for testing or development.	• Identify the document requiring that Live PANs are not used for: i. Testing ii. Development • Identify the responsible development personnel interviewed who confirm that Live PANs are not used for: i. Testing ii. Development • Describe how the observed application confirms that live PANs are not used for: i. Testing ii. Development		✓	✓	✓	
5.1.2 Removal of test data and accounts before release to customer. ***Aligns with PCI DSS Requirement 6.4.4***	**5.1.2** Test data and accounts are removed before release to customer.	• Identify the document that defines processes for: i. Removing test data before release to customer ii. Removing test accounts before release to customer • Identify the responsible development personnel interviewed who confirm that: i. Test data are removed before the application is released to customers. ii. Test accounts are removed before the application is released to customers. • Describe how the observed application confirms that: i. Test data are removed before the application is released to customers. ii. Test accounts are removed before the application is released to customers.		✓	✓	✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
5.1.3 Removal of custom payment application accounts, user IDs, and passwords before payment applications are released to customers ***Aligns with PCI DSS Requirement 6.3.1***	**5.1.3** Custom payment application accounts, user IDs, and passwords are removed before payment application is released to customers.	• Identify the document defining processes for removing custom accounts, user IDs and passwords before the application is released to customers. • Identify the responsible development personnel interviewed who confirm that custom accounts, user IDs and passwords are removed before the application is released to customers. • Describe how the observed application confirms that custom accounts, user IDs and passwords are removed before the application is released to customers.		✓	✓	✓	
5.1.4 Review of payment application code prior to release to customers after any significant change, to identify any potential coding vulnerability. ***Note:*** *This requirement for code reviews applies to all payment application components (both internal and public-facing web applications), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties.* ***Aligns with PCI DSS Requirement 6.3.2***	**5.1.4** Confirm the vendor performs code reviews for all significant application code changes (either using manual or automated processes), as follows: ▪ Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. ▪ Code reviews ensure code is developed according to secure coding guidelines. (See PA-DSS Requirement 5.2.) ▪ Appropriate corrections are implemented prior to release. ▪ Code review results are reviewed and approved by management prior to release.	• Describe the documented processes used for performing code reviews (for example, manual or automated, or a combination of both). • Identify the document defining the processes for application code reviews, and confirm the documented processes include the following: i. Code changes must be reviewed by individuals other than the original author. ii. Code changes must be reviewed by individuals who are knowledgeable in: ○ Code review techniques. ○ Secure coding practices. iii. Code reviews must ensure secure coding guidelines have been followed. iv. Any corrections identified during the code review must be implemented prior to release. v. Code review results must be reviewed by management prior to release. vi. Code review results must be approved by management prior to release.		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
		• Identify the responsible personnel interviewed who confirm that: i. Code changes are reviewed by individuals other than the original author. ii. Code changes are reviewed by individuals who are knowledgeable in: ○ Code review techniques. ○ Secure coding practices. iii. Code reviews ensure secure coding guidelines have been followed. iv. Any corrections identified during the code review are implemented prior to release. v. Code review results are reviewed by management prior to release. vi. Code review results are approved by management prior to release. • Describe how each of the following were observed to be implemented: i. Code changes are reviewed by individuals other than the original author. ii. Code changes are reviewed by individuals who are knowledgeable in: ○ Code review techniques. ○ Secure coding practices. iii. Code reviews ensure secure coding guidelines have been followed. iv. Any corrections identified during the code review are implemented prior to release. v. Code review results are reviewed by management prior to release. vi. Code review results are approved by management prior to release.			✓	✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
5.2 Develop all payment applications (internal and external, and including web administrative access to product) based on secure coding guidelines. Cover prevention of common coding vulnerabilities in software development processes, to include: ***Note:*** *The vulnerabilities listed in PA-DSS Requirements 5.2.1 through 5.2.9 and in PCI DSS at 6.5.1 through 6.5.9 were current with industry best practices when* this version of *PA DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.* ***Aligns with PCI DSS Requirement 6.5***	**5.2.a** Obtain and review software development processes for payment applications (internal and external, and including web-administrative access to product). Verify the process includes training in secure coding techniques for developers, based on industry best practices and guidance.	• Identify the documented software development processes, which include training in secure coding techniques for developers, for all payment applications, based on industry best practices and guidance. • Identify the industry best practice and guidance being followed.		✓			
	5.2.b Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.	• Identify the sample of developers interviewed. • Describe how the interviewed personnel demonstrated they are knowledgeable in secure coding techniques.			✓		✓
	5.2.c Verify that payment applications are not vulnerable to common coding vulnerabilities by performing manual or automated penetration testing that specifically attempts to exploit each of the following:	• Describe the penetration testing techniques used, including whether manual or automated (or both) testing was performed.				✓	
5.2.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws	**5.2.1** Injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.)	• Describe how the application was tested for vulnerability to injection flaws, particularly SQL injection. • Describe how results of the penetration testing results confirm the application is not vulnerable to injection flaws, particularly SQL injection.				✓	
5.2.2 Buffer Overflow	**5.2.2** Buffer Overflow (Validate buffer boundaries and truncate input strings.)	• Describe how the application was tested for vulnerability to buffer overflow. • Describe how results of the penetration testing results confirm the application is not vulnerable to buffer overflow.				✓	
5.2.3 Insecure cryptographic storage	**5.2.3** Insecure cryptographic storage (Prevent cryptographic flaws.)	• Describe how the application was tested for vulnerability to insecure cryptographic storage. • Describe how results of the penetration testing results confirm the application is not vulnerable to insecure cryptographic storage.				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
5.2.4 Insecure communications	**5.2.4** Insecure communications (Properly encrypt all authenticated and sensitive communications.)	• Describe how the application was tested for vulnerability to insecure communications. • Describe how results of the penetration testing results confirm the application is not vulnerable to insecure communications.				✓	
5.2.5 Improper error handling	**5.2.5** Improper error handling (Do not leak information via error messages)	• Describe how the application was tested for vulnerability to improper error handling. • Describe how results of the penetration testing results confirm the application is not vulnerable to improper error handling.				✓	
5.2.6 All "High" vulnerabilities as identified in the vulnerability identification process at PA-DSS Requirement 7.1	**5.2.6** All "High" vulnerabilities as identified in PA-DSS Requirement 7.1	• Describe how the application was tested for "high vulnerabilities." • Describe how results of the penetration testing results confirm the application is not vulnerable to the "High" vulnerabilities which were tested				✓	
Note: *Requirements 5.2.7 through 5.2.9, below, apply to web-based applications and application interfaces (internal or external):*							
5.2.7 Cross-site scripting (XSS)	**5.2.7** Cross-site scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.)	• Describe how the application was tested for vulnerability to cross-site scripting (XSS). • Describe how results of the penetration testing results confirm the application is not vulnerable to cross-site scripting (XSS).				✓	
5.2.8 Improper Access Control such as insecure direct object references, failure to restrict URL access, and directory traversal)	**5.2.8** Insecure direct object references (Properly authenticate users and sanitize input. Do not expose internal object references to users.)	• Describe how the application was tested for vulnerability to insecure direct object references. • Describe how results of the penetration testing results confirm the application is not vulnerable to insecure direct object references.				✓	
5.2.9 Cross-site request forgery (CSRF)	**5.2.9** Cross-site request forgery (CSRF) (Do not reply on authorization credentials and tokens automatically submitted by browsers.)	• Describe how the application was tested for vulnerability to cross-site request forgery (CSRF). • Describe how results of the penetration testing results confirm the application is not vulnerable to cross-site request forgery (CSRF).				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
5.3 Software vendor must follow change control procedures for all product software configuration changes. The procedures must include the following: ***Aligns with PCI DSS Requirement 6.4.5***	**5.3.a** Obtain and examine the vendor's change-control procedures for software modifications, and verify that the procedures require items 5.3.1–5.3.4 below.	• Identify the document which contains the vendor's change-control procedures for software modifications. • Confirm the documented procedures require the following for all changes: i. Documentation of customer impact ii. Documented approval by authorized parties iii. Functionality testing to ensure the change does not adversely impact the security of the system iv. Testing of all updates for compliance with PA-DSS Requirement 5.2 (to address the vulnerabilities identified in 5.2.1 – 5.2.9) v. Back-out or de-installation procedures		✓			
	5.3.b Examine recent payment application changes, and trace those changes back to related change control documentation. Verify that, for each change examined, the following was documented according to the change control procedures:	• Identify the recent payment application changes examined for Requirements 5.3.1 through 5.3.4 below. • Describe how the changes were traced back to the related change control documentation.					✓
5.3.1 Documentation of impact	**5.3.1** Verify that documentation of customer impact is included in the change control documentation for each change.	• For each examined change, describe how documentation of customer impact is included in the change control documentation.		✓			
5.3.2 Documented approval of change by appropriate authorized parties	**5.3.2** Verify that documented approval by appropriate authorized parties is present for each change.	• For each examined change, describe how documented approval by appropriate authorized parties is present in the change control documentation.		✓			
5.3.3 Functionality testing to verify that the change does not adversely impact the security of the system.	**5.3.3.a** For each sampled change, verify that functionality testing was performed to verify that the change does not adversely impact the security of the system	• For each examined change: i. Describe how details of the functionality testing performed are included in the change control documentation. ii. Describe how the documented functionality testing verifies that the change did not adversely impact the security of the system.		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	5.3.3.b Verify that all changes (including patches) are tested for compliance with 5.2 before being released.	• For each sampled change: i. Describe how details of testing for compliance with PA-DSS Requirement 5.2 (to address the vulnerabilities defined in 5.2.1 – 5.2.9) are included in the change control documentation. ii. Describe how the documented testing verifies that the change is compliant with PA-DSS Requirement 5.2 (that the vulnerabilities in 5.2.1 – 5.2.9 are addressed).		✓			
5.3.4 Back-out or product de-installation procedures	**5.3.4** Verify that back-out or product de-installation procedures are prepared for each change.	• For each examined change, describe how back-out or de-installation procedures are included in the change control documentation		✓			
5.4 The payment application must only use or require use of necessary and secure services, protocols, daemons, components, and dependent software and hardware, including those provided by third parties, for any functionality of the payment application (for example, if NetBIOS, file-sharing, Telnet, FTP, etc., are required by the application, they are secured via SSH, S-FTP, SSL, IPSec, or other technology). ***Aligns with PCI DSS Requirement 2.2.2***	**5.4.a** Examine system services, protocols, daemons, components, and dependent software and hardware enabled or required by the payment application. Verify that only necessary and secure services, protocols, daemons, components, dependent software and hardware are enabled by default "out of the box."	• Describe how the following were identified: i. All system services enabled or required by the payment application ii. All protocols enabled or required by the payment application iii. All daemons enabled or required by the payment application iv. All components enabled or required by the payment application v. All dependent software enabled or required by the payment application vi. All dependent hardware enabled or required by the payment application • Describe how each identified system service, protocol, daemon, component, dependent software and dependent hardware was observed to be: i. Necessary ii. Secure • Describe how only necessary and secure services, protocols, daemons, components, dependent software and dependent hardware were observed to be enabled by default "out of the box."	✓			✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	5.4.b If the application supports any insecure services, daemons, protocols or components, verify they are securely configured by default "out of the box."	• Identify whether the application supports any insecure: i. Services ii. Daemons iii. Protocols iv. Components • For each identified insecure service, daemon, protocol or component, describe how each was observed to be securely configured by default "out of the box."	✓			✓	
	5.4.c Verify that the *PA-DSS Implementation Guide* documents all required protocols, services, components, and dependent software and hardware that are necessary for any functionality of the payment application, including those provided by third parties.	• For each of the following, briefly describe how the *PA-DSS Implementation Guide* documents all that are required for any functionality of the payment application (as identified in Requirement 5.4.a): i. Protocols ii. Services iii. Components iv. Dependent software v. Dependent hardware • For each of the following, briefly describe how the *PA-DSS Implementation Guide* documents all that are provided by third parties for any functionality of the payment application: i. Protocols ii. Services iii. Components iv. Dependent software v. Dependent hardware		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 6: Protect wireless transmissions							
6.1 For payment applications using wireless technology, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. The wireless technology must be implemented securely. ***Aligns with PCI DSS Requirements 1.2.3 & 2.1.1***	**6.1** For payment applications developed by the vendor using wireless technology, and other wireless applications bundled with the payment application, verify that the wireless applications do not use vendor default settings, as follows:	• Identify whether the payment application uses wireless technologies. • Identify whether other applications bundled with the payment application use wireless technologies.				✓	
	6.1.a Verify encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions	*If the application uses wireless technology, or wireless applications are bundled with the payment application*: • Describe how observed wireless settings confirm that default encryption keys have been changed • Describe the processes observed to ensure: i. Encryption keys are changed from default at installation. ii. Encryption keys are changed whenever anyone with knowledge of the keys: ○ Leaves the company ○ Changes position	✓			✓	
	6.1.b Verify default SNMP community strings on wireless devices were changed	• Describe how observed wireless settings confirm that default SNMP community strings are changed.	✓				
	6.1.c Verify default passwords/passphrases on access points were changed	• Describe how observed wireless settings confirm that default passwords/passphrases are changed.	✓				
	6.1.d Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks	• Describe how observed wireless settings confirm that firmware is updated to support strong encryption over wireless networks for: i. Authentication ii. Transmission	✓				

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	6.1.e Verify other security-related wireless vendor defaults were changed, if applicable	• Identify any other security-related wireless vendor defaults. • Describe how observed wireless settings confirm these defaults are changed.	✓			✓	
	6.1.f Examine the *PA-DSS Implementation Guide* prepared by the vendor to verify that customers and resellers/integrators are instructed, if wireless is used, to: ▪ Change wireless vendor defaults as defined in 6.1.a – 6.1.e above; ▪ Install a firewall between any wireless networks and systems that store cardholder data, and ▪ Configure firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment	• Briefly describe how the PA-DSS Implementation Guide provides instructions for customers and resellers/integrators that: i. Encryption keys must be changed from default at installation. ii. Encryption keys must be changed anytime anyone with knowledge of the keys: o Leaves the company o Changes positions iii. Default SNMP community strings on wireless devices must be changed. iv. Default passwords/passphrases on access points must be changed. iii. Firmware on wireless devices must be updated to support strong encryption for: o Authentication o Transmission iv. Other security-related wireless vendor defaults must be changed. v. A firewall must be installed between any wireless networks and systems that store cardholder data. vi. Firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
6.2 For payment applications using wireless technology, payment application must facilitate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. ***Note:*** *The use of WEP as a security control was prohibited as of 30 June 2010.* ***Aligns with PCI DSS Requirement 4.1.1***	**6.2.a** For payment applications developed by the vendor using wireless technology, and other wireless applications bundled with the vendor application, verify that industry best practices (for example, IEEE 802,11.i) were used to include or make available strong encryption for authentication and transmission.	• If the application uses wireless technology, or wireless applications are bundled with the payment application: i. Identify the industry best practices used to include or make available strong encryption for: ○ Authentication ○ Transmission ii. Describe how the identified best practices were observed to have been implemented for: ○ Authentication ○ Transmission				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	6.2.b If customers could implement the payment application into a wireless environment, examine *PA-DSS Implementation Guide* prepared by the vendor to verify customers and resellers/integrators are instructed on PCI DSS-compliant wireless settings, including changing wireless vendor defaults (per 6.1.a – 6.1.e above), and using industry best practices to implement strong encryption for authentication and transmission of cardholder data (per 6.2.a).	• Identify whether the application could be implemented into a wireless environment.				✓	
		• If the application *cannot be* implemented into a wireless environment, describe how the application was observed to prevent such implementation.				✓	
		• If the application *could be* implemented into a wireless environment, briefly describe how the PA-DSS Implementation Guide provides instructions that: i. Encryption keys must be changed from default at installation. ii. Encryption keys must be changed anytime anyone with knowledge of the keys ○ Leaves the company ○ Changes positions iii. Default SNMP community strings on wireless devices must be changed. iv. Default passwords/passphrases on access points must be changed. v. Firmware on wireless devices must be updated to support strong encryption for: ○ Authentication ○ Transmission vi. Other security-related wireless vendor defaults must be changed. vii. Industry best practices must be used to implement strong encryption for: ○ Authentication ○ Transmission		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 7: Test payment applications to address vulnerabilities							
7.1 Software vendors must establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities and to test their payment applications for vulnerabilities. Any underlying software or systems that are provided with or required by the payment application (for example, web servers, third-party libraries and programs) must be included in this process. ***Aligns with PCI DSS Requirement 6.2*** ***Note:*** *Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical component of the application.*	**7.1** Obtain and examine processes to identify new vulnerabilities and to test payment applications for new vulnerabilities. Verify the processes include the following:						
	7.1.a Verify that processes include assigning a risk ranking to identified vulnerabilities. (At minimum, the most critical, highest risk vulnerabilities should be ranked as "High.")	• Identify the document defining the processes for assigning risk rankings to identified vulnerabilities. • Briefly describe the process for assigning risk rankings to identified vulnerabilities. (At a minimum, the most critical, highest risk vulnerabilities should be ranked as "High.") • Describe how risk rankings were observed to be assigned to vulnerabilities.		✓		✓	
	7.1.b Verify the processes to identify new security vulnerabilities include using outside sources for security vulnerability information	• Identify the documented processes that include using outside sources for security vulnerability information. • Briefly describe how new security vulnerabilities are identified. • Describe how outside sources were observed to be used to identify new security vulnerabilities. • Identify the outside sources used for security vulnerability information.		✓		✓	
	7.1.c Verify that processes include testing of payment applications for new vulnerabilities	• Identify the documented processes that include testing of payment applications for new vulnerabilities. • Describe how payment applications were observed to be tested for new vulnerabilities.		✓		✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	7.1.d Verify that processes to identify new vulnerabilities and implement corrections into payment application apply to all software provided with or required by the payment application (for example, web servers, third-party libraries and programs).	• Identify the document that requires processes to identify new vulnerabilities and implement corrections apply to: i. All software provided with the payment application ii. All software required by the payment application • Describe how the processes were observed to identify new vulnerabilities for: i. All software provided with the payment application ii. All software required by the payment application • Describe how the processes were observed to implement corrections for: i. All software provided with the payment application ii. All software required by the payment application		✓		✓	
7.2 Software vendors must establish a process for timely development and deployment of security patches and upgrades, which includes delivery of updates and patches in a secure manner with a known chain-of-trust, and maintenance of the integrity of patch and update code during delivery and deployment.	**7.2.a** Obtain and examine processes to develop and deploy security patches and upgrades for software. Verify that processes include the timely development and deployment of patches to customers	• Identify the document that defines processes for: i. Developing security patches and upgrades ii. Deploying security patches and upgrades • Briefly describe the processes for: i. Timely development of security patches and upgrades ii. Timely deployment of security patches and upgrades to customers • Describe how the following were observed to be implemented: i. Timely development of security patches and upgrades ii. Timely deployment of security patches and upgrades to customers		✓		✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	7.2.b Review processes to verify that patches and updates are delivered in a secure manner with a known chain-of-trust	• Identify the document that defines processes for: i. Delivering patches and updates in a secure manner ii. Delivering patches and updates with a known chain-of-trust • Describe how patches and updates were observed to be delivered: i. In a secure manner ii. With a known chain-of-trust		✓		✓	
	7.2.c Review processes to verify that patches and updates are delivered in a manner that maintains the integrity of the deliverable	• Identify the document that defines processes for delivering patches and updates in a manner that maintains the integrity of the deliverable. • Describe how the integrity of the deliverable was observed to be maintained.		✓		✓	
	7.2.d Review processes to verify that patches and updates are integrity tested on the target system prior to installation	• Identify the document that defines processes for integrity testing of patches and updates on the target system prior to installation. • Describe how the integrity of patches and upgrades was observed to be verified on the target system prior to installation.		✓		✓	
	7.2.e To verify that the integrity of patch and update code is maintained, run the update process with arbitrary code and determine that the system will not allow the update to occur.	• Describe how the update process was run with arbitrary code. • Describe how it was determined that the system will not allow the update to occur.				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 8: Facilitate secure network implementation							
8.1 The payment application must be able to be implemented into a secure network environment. Application must not interfere with use of devices, applications, or configurations required for PCI DSS compliance (for example, payment application cannot interfere with anti-virus protection, firewall configurations, or any other device, application, or configuration required for PCI DSS compliance). ***Aligns with PCI DSS Requirements 1, 3, 4, 5, and 6***	**8.1** Test the payment application in a lab to obtain evidence that it can run in a network that is fully compliant with PCI DSS. Verify that the payment application does not inhibit installation of patches or updates to other components in the environment.	• Briefly describe how the test network was verified to be fully compliant with PCI DSS. • Describe how the payment application was observed to run in the PCI DSS compliant network. • Describe how the payment application was observed to not interfere with use of devices, applications, or configurations required for PCI DSS compliance (for example, anti-virus protection, firewall configurations, or any other device, application, or configuration required for PCI DSS compliance). • Describe how the payment application was observed to not inhibit installation of patches or updates to other components in the environment.				✓	
Requirement 9: Cardholder data must never be stored on a server connected to the Internet							
9.1 The payment application must be developed such that a database server and web server are not required to be on the same server, nor is a database server required to be in the DMZ with the web server. ***Aligns with PCI DSS Requirement 1.3.7***	**9.1.a** To verify that the payment application stores cardholder data in the internal network, and never in the DMZ, obtain evidence that the payment application does not require data storage in the DMZ, and will allow use of a DMZ to separate the Internet from systems storing cardholder data (for example, payment application must not require that a database server and web server be on the same server, or in the DMZ with the web server).	• Describe how the payment application was observed to not require that a database server be on the same server as a web server. • Describe how the payment application was observed to not require a database server to be in the DMZ with the web server. • Describe how the payment application was observed to allow use of a DMZ to separate the Internet from systems storing cardholder data.				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
	9.1.b If customers could store cardholder data on a server connected to the Internet, examine *PA-DSS Implementation Guide* prepared by vendor to verify customers and resellers/integrators are instructed not to store cardholder data on Internet-accessible systems (for example, web server and database server must not be on same server).	• Briefly describe how the *PA-DSS Implementation Guide* instructs customers and resellers/integrators to not store cardholder data on Internet-accessible systems.				✓	
Requirement 10: Facilitate secure remote access to payment application							
10.1 The payment application must not interfere with use of two-factor authentication technologies for secure remote access. (For example, RADIUS with tokens, TACACS with tokens, or other technologies that facilitate two-factor authentication.) ***Note:*** *Two-factor authentication requires that two of the three authentication methods (see below) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication. The authentication methods, also known as a factors, are:* ▪ *Something you know, such as a password or passphrase* ▪ *Something you have, such as a token device or smart card* ▪ *Something you are, such as a biometric* ***Aligns with PCI DSS Requirement 8.3***	**10.1** Test the payment application in a lab to obtain evidence that it does not interfere with two-factor authentication technologies.	• Briefly describe how the payment application was tested with two-factor authentication technologies. • Describe the two-factor authentication technologies used in the testing, and identify which two factors were used: ○ Something you know ○ Something you are ○ Something you have • Describe how results of the testing verify the payment application does not interfere with the use of two-factor authentication technologies.				✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
10.2 If the payment application may be accessed remotely, remote access to the payment application must be authenticated using a two-factor authentication mechanism. ***Note:*** *Two-factor authentication requires that two of the three authentication methods be used for authentication (see PA-DSS Req. 10.1 for descriptions of authentication methods).* ***Aligns with PCI DSS Requirement 8.3***	**10.2** If the payment application may be accessed remotely, examine *PA-DSS Implementation Guide* prepared by the software vendor, and verify it contains instructions for customers and resellers/integrators regarding required use of two-factor authentication (two of the three authentication methods described in PA DSS Req. 10.1).	• Identify whether the payment application may be accessed remotely.				✓	
		• If the payment application <u>*cannot be*</u> accessed remotely, describe how the application was observed to prevent such access.				✓	
		• If the payment application <u>*could be*</u> accessed remotely, briefly describe how the *PA-DSS Implementation Guide* provides instructions for customers and resellers/integrators regarding required use of two-factor authentication.		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
10.3 Any remote access into the payment application must be done securely, as follows:	**10.3** Verify that any remote access is done as follows:						
10.3.1 If payment application updates are delivered via remote access into customers' systems, software vendors must tell customers to turn on remote-access technologies only when needed for downloads from vendor, and to turn off immediately after download completes. Alternatively, if delivered via VPN or other high-speed connection, software vendors must advise customers to properly configure a firewall or a personal firewall product to secure "always-on" connections. ***Aligns with PCI DSS Requirements 1 and 12.3.9***	**10.3.1** If the vendor delivers payment application and/or updates via remote access to customer networks, examine *PA-DSS Implementation Guide* prepared by vendor, and verify it contains: ▪ Instructions for customers and resellers/integrators regarding secure use of remote-access technologies, specifying that remote-access technologies used by vendors and business partners should be activated only when needed and immediately deactivated after use. ▪ Recommendation for customers and resellers/ integrators to use a securely configured firewall or a personal firewall product if computer is connected via VPN or other high-speed connection, to secure these "always-on" connections, per PCI DSS Requirement 1.	• Identify whether payment application updates are delivered via remote access into customers' systems.				✓	
		• If payment application updates are delivered via remote access into customers' systems, briefly describe how the *PA-DSS Implementation Guide* includes the following: i. Instructions regarding secure use of remote-access technologies, including that remote-access technologies used by vendors and business partners should be: ○ Activated only when needed ○ Immediately deactivated after use ii. Recommendation to use a securely configured firewall or a personal firewall product if computer is connected via VPN or other high-speed connection to secure these "always-on" connections per PCI DSS Requirement 1.		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
10.3.2 If vendors, resellers/integrators, or customers can access customers' payment applications remotely, the remote access must be implemented securely. ***Note:*** *Examples of remote access security features include*: ▪ *Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).* ▪ *Allow connections only from specific (known) IP/MAC addresses.* ▪ *Use strong authentication and complex passwords for logins (See PA-DSS Requirements. 3.1.1 through 3.1.1.0)* ▪ *Enable encrypted data transmission according to PA-DSS Requirement 12.1.* ▪ *Enable account lockout after a certain number of failed login attempts. (See PA-DSS Requirement 3.1.8.)* ▪ *Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed.* ▪ *Enable the logging function.* ▪ *Restrict access to customer passwords to authorized reseller/integrator personnel.* ▪ *Establish customer passwords according to PA-DSS Requirements 3.1.1through 3.1.10.* ***Aligns with PCI DSS Requirement 8.3***	**10.3.2.a** If the software vendor uses remote access products for remote access to the customers' payment application, verify that vendor personnel implement and use remote access security features.	• Identify whether the software vendor uses remote access products for remote access to the customers' payment application. • If the software vendor does use remote access products for remote access to the customer's payment application: i. Identify the remote security features that are implemented. ii. For each remote security feature identified: ○ Describe how that security feature was observed to be implemented. ○ Identify the responsible personnel interviewed who confirm that the security feature is used.			✓	✓	
	10.3.2.b If resellers/integrators or customers can use remote access software, examine *PA-DSS Implementation Guide* prepared by the software vendor, and verify that customers and resellers/integrators are instructed to use and implement remote access security features.	• Identify whether or not resellers/integrators or customers can use remote access software.				✓	
		• If the resellers/integrators or customers <u>*cannot use*</u> remote access software, describe how use of such software is prevented.				✓	
		• If resellers/integrators or customers <u>*could use*</u> remote access software, briefly describe how the *PA-DSS Implementation* Guide instructs customers and resellers/integrators to: i. Implement remote access security features. ii. Use remote access security features.		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 11: Encrypt sensitive traffic over public networks							
11.1 If the payment application sends, or facilitates sending, cardholder data over public networks, the payment application must support use of strong cryptography and security protocols (for example, SSL/TLS, Internet protocol security (IPSEC), SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS are:* ▪ *The Internet* ▪ *Wireless technologies* ▪ *Global System for Mobile Communications (GSM)* ▪ *General Packet Radio Service (GPRS)* ***Aligns with PCI DSS Requirement 4.1***	**11.1.a** If the payment application sends, or facilitates sending, cardholder data over public networks, verify that strong cryptography and security protocols are provided, or that use thereof is specified.	• Identify whether the payment application sends or facilitates sending cardholder data over public networks.				✓	
		• If the payment application *does not* send, or facilitate sending of, cardholder data over public networks, describe what measures are in place to prevent this.				✓	
		• If the payment application *does* send, or facilitate sending, cardholder data over public networks: i. Identify the strong cryptography provided with the payment application ii. Identify the security protocols provided with the payment application *Or:* i. Identify the strong cryptography specified for use ii. Identify the security protocols specified for use iii. Describe how use of strong cryptography and security protocols is specified		✓		✓	
	11.1.b If the payment application allows data transmission over public networks, examine *PA-DSS Implementation Guide* prepared by the vendor, and verify the vendor includes directions for customers and resellers/integrators to use strong cryptography and security protocols.	• Identify whether the payment application allows data transmission over public networks.				✓	
		• If the payment application *does not* allow data transmission over public networks, describe how the application was observed to prevent such transmissions.				✓	
		• If the payment application *does* allow data transmission over public networks, briefly describe how the *PA-DSS Implementation Guide* includes directions for customers and resellers/integrators to: i. Use strong cryptography ii. Use security protocols		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
11.2 If the payment application facilitates sending of PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat), the payment application must provide a solution that renders the PAN unreadable or implements strong cryptography, or specify use of strong cryptography to encrypt the PANs. ***Aligns with PCI DSS Requirement 4.2***	**11.2.a** If the payment application allows and/or facilitates sending of PANs by end-user messaging technologies, verify that a solution that renders the PAN unreadable or implements strong cryptography is provided, or that use thereof is specified.	• Identify whether the payment application allows and/or facilitates the sending of PANs by end-user messaging technologies.				✓	
		• If the payment application ***does not*** allow and/or facilitate sending of PANs by end-user messaging technologies, describe how the application was observed to prevent such action.				✓	
		• If the payment application ***does*** allow and/or facilitate the sending of PANs by end-user messaging technologies: i. Identify the solution provided with the application that: ○ Renders the PAN unreadable, *or* ○ Implements strong cryptography *Or:* i. Identify and describe the solution specified for use that: ○ Implements strong cryptography, *or* ○ Renders PAN unreadable ii. Describe how use of the solution is specified.		✓		✓	
	11.2.b If the payment application allows and/or facilitates the sending of PANs by end-user messaging technologies, examine *PA-DSS Implementation Guide* prepared by the vendor, and verify the vendor includes directions for customers and resellers/integrators to use a solution that renders the PAN unreadable or implements strong cryptography.	• If the payment application allows and/or facilitates the sending of PANs by end-user messaging technologies, briefly describe how the *PA-DSS Implementation Guide* includes directions for customers and resellers/integrators to: i. Use a solution that renders the PAN unreadable, or ii. Use a solution that implements strong cryptography		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
Requirement 12: Encrypt all non-console administrative access							
12.1 Instruct customers to encrypt all non-console administrative access with strong cryptography, using technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. ***Note:*** *Telnet or rlogin must never be used for administrative access.* ***Aligns with PCI DSS Requirement 2.3***	**12.1** If payment application or server allows non-console administration, examine the *PA-DSS Implementation Guide* prepared by vendor, and verify vendor recommends use of strong cryptography, using technologies such as SSH, VPN, or SSL/TLS for encryption of non-console administrative access.	• Identify whether the payment application allows non-console administration. • Identify whether the server allows non-console administration.				✓	
		• If the payment application or server <u>*does not*</u> allow non-console administration: i. Describe the technical constraints observed in the payment application to prevent non-console administration, and/or ii. Describe the technical constraints on the server observed to prevent non-console administration.				✓	
		• If the payment application or server <u>*does*</u> allow non-console administration: i. Briefly describe how the *PA-DSS Implementation Guide* provides detailed instructions for using of strong cryptography for encryption of non-console administrative access.		✓			
Requirement 13: Maintain instructional documentation and training programs for customers, resellers, and integrators							
13.1 Develop, maintain, and disseminate a *PA-DSS Implementation Guide(s)* for customers, resellers, and integrators that accomplishes the following:	**13.1** Examine the *PA-DSS Implementation Guide* and related processes, and verify the guide is disseminated to all relevant payment application users (including customers, resellers, and integrators).	• Describe how the *PA-DSS Implementation Guide* is developed, maintained and disseminated to all relevant payment application users, including customers, resellers and integrators. • Describe how these processes were observed to be implemented.		✓		✓	
13.1.1 Addresses all requirements in this document wherever the *PA-DSS Implementation Guide* is referenced.	**13.1.1** Verify the *PA-DSS Implementation Guide* covers all related requirements in this document.	• Describe how the *PA-DSS Implementation Guide* was verified to cover all related requirements in this document.		✓			

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
13.1.2 Includes a review at least annually and updates to keep the documentation current with all major and minor software changes as well as with changes to the requirements in this document.	**13.1.2.a** Verify the *PA-DSS Implementation Guide* is reviewed on an annual basis and updated as needed to document all major and minor changes to the payment application.	• Describe the processes observed and review updates to the *PA-DSS Implementation Guide* to ensure: i. The *PA-DSS Implementation Guide* is reviewed at least annually for changes to the payment application. ii. The *PA-DSS Implementation Guide* is updated as needed to document: ○ All major changes to the payment application ○ All minor changes to the payment application		✓		✓	
	13.1.2.b Verify the *PA-DSS Implementation Guide* is reviewed on an annual basis and updated as needed to document changes to the PA-DSS requirements.	• Describe the processes observed and review updates to the *PA-DSS Implementation Guide* to ensure: i. The *PA-DSS Implementation Guide* is reviewed at least annually for changes to the PA-DSS requirements. ii. The *PA-DSS Implementation Guide* is updated as needed to document changes to the PA-DSS requirements.		✓		✓	
13.2 Develop and implement training and communication programs to ensure payment application resellers and integrators know how to implement the payment application and related systems and networks according to the *PA-DSS Implementation Guide* and in a PCI DSS-compliant manner.	**13.2** Examine the training materials and communication program for resellers and integrators, and confirm the materials cover all items noted for the *PA-DSS Implementation Guide* throughout this document.	• Describe the training and communication programs observed to be implemented for resellers and integrators. • Describe how the observed training materials and communication programs were confirmed to cover all items in the *PA-DSS Implementation Guide.* • Describe how the observed training materials and communication programs ensure that resellers and integrators know how to implement the following in a PCI DSS-compliant manner: i. The payment application ii. Related systems and networks		✓		✓	

PA-DSS 2.0 Requirements	Testing Procedures	Reporting Details	Reporting Methodology				
			Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state	Identify sample
13.2.1 Update the training materials on an annual basis and whenever new payment application versions are released.	**13.2.1.a** Examine the training materials for resellers and integrators and verify the materials are reviewed on an annual basis and when new payment application versions are released, and updated as needed.	• Describe how the training materials were observed to be reviewed: i. On an annual basis ii. When new versions of the payment application are released • Describe how the training materials were observed to be updated as needed: i. On an annual basis ii. When new versions of the payment application are released		✓		✓	
	13.2.1.b Examine the distribution process for new payment application versions and verify that updated documentation is distributed with the updated payment application.	• Briefly describe the distribution process for new payment application versions. • Describe how updated documentation was observed to be distributed with the updated payment application.				✓	
	13.2.1.b Select a sample of resellers and integrators and interview them to verify they received the training materials.	• Identify the sample of resellers and integrators interviewed. • For each reseller and integrator in the sample: i. Identify the interviewed personnel. ii. Describe how the interviewed personnel received the training materials.			✓		✓