Payment Card Industry (PCI)

Payment Application Data Security Standard

Requirements and Security Assessment Procedures

Version 2.0

October 2010

Document Changes

Date	Version	Description	Pages
October 1, 2008	*1.2*	*To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.*	
July 2009	*1.2.1*	*Under "Scope of PA-DSS," align content with the* PA-DSS Program Guide, v1.2.1, *to clarify applications to which PA-DSS applies.*	*v, vi*
		Under Laboratory Requirement 6, corrected spelling of "OWASP."	*30*
		In the Attestation of Validation, Part 2a, update Payment Application Functionality to be consistent with the application types listed in the PA-DSS Program Guide, *and clarify annual re-validation procedures in Part 3b.*	*32, 33*
October 2010	*2.0*	*Update and implement minor changes from v1.2.1 and align with new PCI DSS v2.0. For details, please see* "PA-DSS—Summary of Changes from PA-DSS Version 1.2.1 to 2.0.*"*	

Copyright 2010 PCI Security Standards Council LLC

Table of Contents

Document Changes **2**

Introduction **4**

Purpose of This Document 4
Relationship between PCI DSS and PA-DSS 4
Scope of PA-DSS 5
PA-DSS Applicability to Payment Applications on Hardware Terminals 6
Roles and Responsibilities 8
PA-DSS Implementation Guide 10
Payment Application Qualified Security Assessor (PA-QSA) Requirements 10
Testing Laboratory 11

PCI DSS Applicability Information **12**

Instructions and Content for Report on Validation **14**

PA-DSS Completion Steps **16**

PA-DSS Program Guide **16**

PA-DSS Requirements and Security Assessment Procedures **17**

1. Do not retain full magnetic stripe, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data 17
2. Protect stored cardholder data 21
3. Provide secure authentication features 27
4. Log payment application activity 31
5. Develop secure payment applications 33
6. Protect wireless transmissions 36
7. Test payment applications to address vulnerabilities 38
8. Facilitate secure network implementation 39
9. Cardholder data must never be stored on a server connected to the Internet 39
10. Facilitate secure remote access to payment application. 40
11. Encrypt sensitive traffic over public networks 43
12. Encrypt all non-console administrative access 44
13. Maintain instructional documentation and training programs for customers, resellers, and integrators 44

Appendix A: Summary of Contents for the *PA-DSS Implementation Guide* **46**

Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment **52**

Copyright 2010 PCI Security Standards Council LLC

Introduction

Purpose of This Document

This document is to be used by Payment Application-Qualified Security Assessors (PA-QSAs) conducting payment application reviews, so that software vendors can validate that a payment application complies with the PCI Payment Application Data Security Standard (PA-DSS). This document is also to be used by PA-QSAs as a template to create the Report on Validation.

Additional resources including Attestations of Validation, Frequently Asked Questions (FAQs) and the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* are available on the PCI Security Standards Council (PCI SSC) website—www.pcisecuritystandards.org.

Relationship between PCI DSS and PA-DSS

Use of a PA-DSS compliant application by itself does not make an entity PCI DSS compliant, since that application must be implemented into a PCI DSS compliant environment and according to the PA-DSS Implementation Guide provided by the payment application vendor (per PA-DSS Requirement 13.1).

The requirements for the Payment Application Data Security Standard (PA-DSS) are derived from the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures*. This document, which can be found at www.pcisecuritystandards.org, details what is required to be PCI DSS compliant (and therefore what a payment application must support to facilitate a customer's PCI DSS compliance).

Traditional PCI Data Security Standard compliance may not apply directly to payment application vendors since most vendors do not store, process, or transmit cardholder data. However, since these payment applications are used by customers to store, process, and transmit cardholder data, and customers are required to be PCI Data Security Standard compliant, payment applications should facilitate, and not prevent, the customers' PCI Data Security Standard compliance. Just a few of the ways payment applications can prevent compliance follow.

1. Storage of magnetic stripe data and/or equivalent data on the chip in the customer's network after authorization;
2. Applications that require customers to disable other features required by the PCI Data Security Standard, like anti-virus software or firewalls, in order to get the payment application to work properly; and
3. Vendors' use of unsecured methods to connect to the application to provide support to the customer.

Secure payment applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of full magnetic stripe data, card verification codes and values (CAV2, CID, CVC2, CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches.

Copyright 2010 PCI Security Standards Council LLC

Scope of PA-DSS

The PA-DSS applies to 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 following guide can be used to determine whether PA-DSS applies to a given payment application:

> ***Note:***
> *All validated payment application products must not be beta versions.*

- PA-DSS does apply to payment applications that are typically sold and installed "off the shelf" without much customization by software vendors.
- PA-DSS does apply to payment applications provided in modules, which typically includes a "baseline" module and other modules specific to customer types or functions, or customized per customer request. PA-DSS may only apply to the baseline module if that module is the only one performing payment functions (once confirmed by a PA-QSA). If other modules also perform payment functions, PA-DSS applies to those modules as well. Note that it is considered a "best practice" for software vendors to isolate payment functions into a single or small number of baseline modules, reserving other modules for non-payment functions. This best practice (though not a requirement) can limit the number of modules subject to PA-DSS.
- PA-DSS does NOT apply to payment applications offered by application or service providers only as a service (unless such applications are also sold, licensed, or distributed to third parties) because:
  1) The application is a service offered to customers (typically merchants) and the customers do not have the ability to manage, install, or control the application or its environment;
  2) The application is covered by the application or service provider's own PCI DSS review (this coverage should be confirmed by the customer); and/or
  3) The application is not sold, distributed, or licensed to third parties.

  Examples of these "software as a service" payment applications include:

  1) Those offered by Application Service Providers (ASP) who host a payment application on their site for their customers' use. Note that PA-DSS would apply, however, if the ASP's payment application were also sold to, and implemented on, a third-party site, and the application was not covered by the ASP's PCI DSS review.
  2) Virtual terminal applications that reside on a service providers' site and are used by merchants to enter their payment transactions. Note that PA-DSS would apply if the virtual terminal application has a portion that is distributed to, and implemented on, the merchant's site, and was not covered by the virtual terminal provider's PCI DSS review.
- PA-DSS does NOT apply to non-payment applications that are part of a payment application suite. Such applications (for example, a fraud-monitoring, scoring or detection application included in a suite) can be, but are not required to be, covered by PA-DSS if the whole suite is assessed together. However, if a payment application is part of a suite that relies on PA-DSS requirements being met by controls in other applications in the suite, a single PA-DSS assessment should be performed for the payment application and all other applications in the suite upon which it relies. These applications should not be assessed separately from other applications they rely upon since all PA-DSS requirements are not met within a single application.

Copyright 2010 PCI Security Standards Council LLC

- PA-DSS does NOT apply to a payment application developed for and sold to a single customer for the sole use of that customer, since this application will be covered as part of the customer's normal PCI DSS compliance review. Note that such an application (which may be referred to as a "bespoke" application) is sold to only one customer (usually a large merchant or service provider), and it is designed and developed according to customer-provided specifications.
- PA-DSS does NOT apply to payment applications developed by merchants and service providers if used only in-house (not sold, distributed, or licensed to a third party), since this in-house developed payment application would be covered as part of the merchant's or service provider's normal PCI DSS compliance.

For example, for the last two bullets above, whether the in-house developed or "bespoke" payment application stores prohibited sensitive authentication data or allows complex passwords would be covered as part of the merchant's or service provider's normal PCI DSS compliance efforts and would not require a separate PA-DSS assessment.

The following list, while not all-inclusive, illustrates applications that are NOT payment applications for purposes of PA-DSS (and therefore do not need to undergo PA-DSS reviews):

- Operating systems onto which a payment application is installed (for example, Windows, Unix)
- Database systems that store cardholder data (for example, Oracle)
- Back-office systems that store cardholder data (for example, for reporting or customer service purposes)

Note: *PCI SSC will ONLY list applications that are payment applications.*

The scope of the PA-DSS review should include the following:

- Coverage of all payment application functionality, including but not limited to 1) end-to-end payment functions (authorization and settlement), 2) input and output, 3) error conditions, 4) interfaces and connections to other files, systems, and/or payment applications or application components, 5) all cardholder data flows, 6) encryption mechanisms, and 7) authentication mechanisms.
- Coverage of guidance the payment application vendor is expected to provide to customers and resellers/integrators (see *PA-DSS Implementation Guide* later in this document) to ensure 1) customer knows how to implement the payment application in a PCI DSS-compliant manner and 2) customer is clearly told that certain payment application and environment settings may prohibit their PCI DSS compliance. Note that the payment application vendor may be expected to provide such guidance even when the specific setting 1) cannot be controlled by the payment application vendor once the application is installed by the customer or 2) is the responsibility of the customer, not the payment application vendor.
- Coverage of all selected platforms for the reviewed payment application version (included platforms should be specified).
- Coverage of tools used by or within the payment application to access and/or view cardholder data (reporting tools, logging tools, etc.)

PA-DSS Applicability to Payment Applications on Hardware Terminals

Payment applications designed to operate on hardware terminals (also known as a standalone or dedicated POS terminal) may undergo a PA-DSS review if the vendor wishes to achieve validation and if PA-DSS compliance requirements can be met. Reasons a vendor may wish to undergo a PA-DSS validation for a payment application on a hardware terminal include, but are not limited to, business needs and compliance

Copyright 2010 PCI Security Standards Council LLC

obligations. This section provides guidance for vendors who wish to gain PA-DSS validation for resident payment applications on hardware terminals.

There are two ways for a resident payment application on a hardware terminal to achieve PA-DSS validation:

1. The resident payment application directly meets all PA-DSS requirements and is validated according to standard PA-DSS procedures.
2. The resident payment application does not meet all PA-DSS requirements, but the hardware that the application is resident on is listed on the PCI SSC's Approved PIN Transaction Security (PTS) Devices List as a current PCI PTS approved Point of Interaction (POI) device. In this scenario, it may be possible for the application to satisfy PA-DSS requirements through a combination of the PA-DSS and PTS validated controls.

The remainder of this section applies only to payment applications that that are resident on a validated PCI PTS approved POI device.

If one or more PA-DSS requirements cannot be met by the payment application directly, they may be satisfied indirectly by controls tested as part of the PCI PTS validation. For a hardware device to be considered for inclusion in a PA-DSS review, the hardware device MUST be validated as a PCI PTS approved POI device and be listed on the PCI SSC's Approved PTS Devices List. The PTS validated POI device, which provides a trusted computing environment, will become a "***required dependency***" for the payment application, and the combination of application and hardware will be listed together on the PA-DSS List of Validation Payment Applications.

When conducting the PA-DSS assessment, the PA-QSA must fully test the payment application with its dependant hardware against all PA-DSS requirements. If the PA-QSA determines that one or more PA-DSS requirements cannot be met by the resident payment application, but they are met by controls validated under PCI PTS, the PA-QSA must:

1. Clearly document which requirements are met as stated per PA-DSS (as usual);
2. Clearly document which requirement was met via PCI PTS in the "In Place" box for that requirement;
3. Include a thorough explanation as to why the payment application could not meet the PA-DSS requirement;
4. Document the procedures that were conducted to determine how that requirement was fully met through a PCI PTS validated control;
5. List the PCI PTS validated hardware terminal as a required dependency in the Executive Summary of the Report on Validation.

Once the PA-QSA's validation of the payment application is complete and is subsequently accepted by the PCI SSC, the PTS validated hardware device will be listed as a dependency for the payment application on the PA-DSS List of Validated Applications.

Resident payment applications on hardware terminals that are validated through a combination of PA-DSS and PCI PTS controls must meet the following criteria:

1. Be provided together to the customer (both hardware terminal and application), OR, if provided separately, the application vendor and/or the reseller/integrator must package the application for distribution such that it will operate only on the hardware terminal it has been validated to run on.
2. Enabled by default to support a customer's PCI DSS compliance.
3. Include ongoing support and updates to maintain PCI DSS compliance.
4. If the application is separately sold, distributed or licensed to customers, the vendor must provide details of the dependant hardware required for use with the application, in accordance with its PA-DSS validation listing.

Copyright 2010 PCI Security Standards Council LLC

Roles and Responsibilities

There are several stakeholders in the payment application community. Some of these stakeholders have a more direct participation in the PA-DSS assessment process—vendors, PA-QSAs and PCI SSC. Other stakeholders that are not directly involved with the assessment process should be aware of the overall process to facilitate their associated business decisions.

The following defines the roles and responsibilities of the stakeholders in the payment application community. Those stakeholders that are involved in the assessment process have those related responsibilities listed.

Payment Brands

American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. are the payment brands that founded the PCI SSC. These payment brands are responsible for developing and enforcing any programs related to PA-DSS compliance, including, but not limited to, the following:

- Any requirements, mandates, or dates for use of PA-DSS compliant payment applications
- Any fines or penalties related to use of non-compliant payment applications

The payment brands may define compliance programs, mandates, dates, etc., using PA-DSS and the validated payment applications listed by PCI SSC. Through these compliance programs, the payment brands promote use of the listed validated payment applications.

Payment Card Industry Security Standards Council (PCI SSC)

PCI SSC is the standards body that maintains the payment card industry standards, including the PCI DSS and PA-DSS. In relation to PA-DSS, PCI SSC:

- Is a centralized repository for PA-DSS Reports of Validation (ROVs)
- Performs Quality Assurance (QA) reviews of PA-DSS ROVs to confirm report consistency and quality
- Lists PA-DSS validated payment applications on the website
- Qualifies and trains PA-QSAs to perform PA-DSS reviews
- Maintains and updates the PA-DSS standard and related documentation according to a standards lifecycle management process

Note that PCI SSC does not approve reports from a validation perspective. The role of the PA-QSA is to document the payment application's compliance to the PA-DSS as of the date of the assessment. Additionally, PCI SSC performs QA to assure that the PA-QSAs accurately and thoroughly document PA-DSS assessments.

Software Vendors

Software vendors ("vendors") develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, and then sell, distribute, or license these payment applications to third parties (customers or resellers/integrators). Vendors are responsible for:

Copyright 2010 PCI Security Standards Council LLC

- Creating PA-DSS compliant payment applications that facilitate and do not prevent their customers' PCI DSS compliance (the application cannot require an implementation or configuration setting that violates a PCI DSS requirement)
- Following PCI DSS requirements whenever the vendor stores, processes or transmits cardholder data (for example, during customer troubleshooting)
- Creating a *PA-DSS Implementation Guide*, specific to each payment application, according to the requirements in this document
- Educating customers, resellers, and integrators on how to install and configure the payment applications in a PCI DSS-compliant manner
- Ensuring payment applications meet PA-DSS by successfully passing a PA-DSS review as specified in this document

PA-QSAs

PA-QSAs are QSAs that have been qualified and trained by PCI SSC to perform PA-DSS reviews.

PA-QSAs are responsible for:

- Performing assessments on payment applications in accordance with the Security Assessment Procedures and the PA-QSA Validation Requirements
- Providing an opinion regarding whether the payment application meets PA-DSS requirements
- Providing adequate documentation within the ROV to demonstrate the payment application's compliance to the PA-DSS
- Submitting the ROV to PCI SSC, along with the Attestation of Validation (signed by both PA-QSA and vendor)
- Maintaining an internal quality assurance process for their PA-QSA efforts

Note: *Not all QSAs are PA-QSAs—there are additional qualification requirements that must be met for a QSA to become a PA-QSA.*

It is the PA-QSA's responsibility to state whether the payment application has achieved compliance. PCI SSC does not approve ROVs from a technical compliance perspective, but performs QA reviews on the ROVs to assure that the reports adequately document the demonstration of compliance.

Resellers and Integrators

Resellers and integrators are those entities that sell, install, and/or service payment applications on behalf of software vendors or others. Resellers and integrators are responsible for:

- Implementing a PA-DSS-compliant payment application into a PCI DSS-compliant environment (or instructing the merchant to do so)
- Configuring the payment application (where configuration options are provided) according to the *PA-DSS Implementation Guide* provided by the vendor
- Configuring the payment application (or instructing the merchant to do so) in a PCI DSS-compliant manner
- Servicing the payment applications (for example, troubleshooting, delivering remote updates, and providing remote support) according to the *PA-DSS Implementation Guide* and PCI DSS

Resellers and integrators do not submit payment applications for assessment. Products may only be submitted by the vendor.

Copyright 2010 PCI Security Standards Council LLC

Customers

Customers are merchants, service providers, or others who buy or receive a third-party payment application to store, process, or transmit cardholder data as part of authorizing or settling of payment transactions. Customers who want to use applications that are compliant with PA-DSS are responsible for:

- Implementing a PA-DSS-compliant payment application into a PCI DSS-compliant environment
- Configuring the payment application (where configuration options are provided) according to the *PA-DSS Implementation Guide* provided by the vendor
- Configuring the payment application in a PCI DSS-compliant manner
- Maintaining the PCI DSS-compliant status for both the environment and the payment application configuration

Note: *A PA-DSS compliant payment application alone is no guarantee of PCI DSS compliance.*

PA-DSS Implementation Guide

Validated payment applications must be capable of being implemented in a PCI DSS-compliant manner. Software vendors are required to provide a *PA-DSS Implementation Guide* to instruct their customers and resellers/integrators on secure product implementation, to document the secure configuration specifics mentioned throughout this document, and to clearly delineate vendor, reseller/integrator, and customer responsibilities for meeting PCI DSS requirements. It should detail how the customer and/or reseller/integrator should enable security settings within the customer's network. For example, the *PA-DSS Implementation Guide* should cover responsibilities and basic features of PCI DSS password security even if this is not controlled by the payment application, so that the customer or reseller/integrator understands how to implement secure passwords for PCI DSS compliance.

Payment applications, when implemented according to the *PA-DSS Implementation Guide*, and when implemented into a PCI DSS-compliant environment, should facilitate and support customers' PCI DSS compliance.

Refer to *Appendix A: Summary of Contents for the PA-DSS Implementation Guide* for a comparison of responsibilities for implementing the controls specified in the *PA-DSS Implementation Guide*.

Payment Application Qualified Security Assessor (PA-QSA) Requirements

Only Payment Application Qualified Security Assessors (PA-QSAs) employed by Qualified Security Assessor (QSA) companies are allowed to perform PA-DSS assessments. Please see the Qualified Security Assessor list at www.pcisecuritystandards.org for a list of companies qualified to perform PA-DSS assessments.

- The PA-QSA must utilize the testing procedures documented in this Payment Application Data Security Standard document.
- The PA-QSA must have access to a laboratory where the validation process is to occur.

Copyright 2010 PCI Security Standards Council LLC

Testing Laboratory

- Testing laboratories can exist in either of two locations: onsite at the PA-QSA location, or onsite at the software vendor's location.
- The testing laboratory should be able to simulate real-world use of the payment application.
- The PA-QSA must validate the clean installation of the lab environment to ensure the environment truly simulates a real world situation and that the vendor has not modified or tampered with the environment in any way.
- Please refer to *Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment* in this document for detailed requirements for the laboratory and related laboratory processes.
- PA-QSA must complete and submit *Appendix B,* completed for the specific laboratory used for the payment application under review, as part of the completed PA-DSS report.

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Applicability Information

(Excerpted from PCI DSS)

The *Payment Card Industry Data Security Standard* (PCI DSS) applies wherever account data is stored, processed or transmitted. *Account Data* consists of *Cardholder Data* plus *Sensitive Authentication Data,* as follows.

Cardholder Data includes:	***Sensitive Authentication Data includes:***
▪ Primary Account Number (PAN) ▪ Cardholder Name ▪ Expiration Date ▪ Service Code	▪ Full magnetic stripe data or equivalent on a chip ▪ CAV2/CVC2/CVV2/CID ▪ PINs/PIN blocks

The primary account number (PAN) is the defining factor in the applicability of PCI DSS requirements and PA-DSS. PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If PAN is not stored, processed, or transmitted, PCI DSS and PA-DSS do not apply.

If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with all PCI DSS requirements ***except*** Requirements 3.3 and 3.4, which apply only to PAN.

PCI DSS represents a minimum set of control objectives which may be enhanced by local, regional and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personally identifiable information or other data elements (for example, cardholder name), or define an entity's disclosure practices related to consumer information. Examples include legislation related to consumer data protection, privacy, identity theft, or data security. PCI DSS does not supersede local or regional laws, government regulations or other legal requirements.

The following table from the *Payment Card Industry Data Security Standard* (PCI DSS) illustrates commonly used elements of cardholder data and sensitive authentication data, whether **storage** of that data is permitted or prohibited, and whether this data needs to be **protected**. This table is not meant to be exhaustive, but is presented to illustrate the different type of requirements that apply to each data element.

Copyright 2010 PCI Security Standards Council LLC

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per PCI DSS Requirement 3.4
Account Data	**Cardholder Data**	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data [1]	Full Magnetic Stripe Data [2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

PCI DSS Requirements 3.3 and 3.4 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4.

PCI DSS ***only applies*** if PANs are stored, processed, and/or transmitted.

[1] *Sensitive authentication data must not be stored after authorization (even if encrypted).*

[2] *Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.*

Copyright 2010 PCI Security Standards Council LLC

Instructions and Content for Report on Validation

This document is to be used by PA-QSAs as the template for creating the Report on Validation. All PA-QSAs must follow instructions in this document for report content and format when completing a Report on Validation.

The Report on Validation should contain the following information as a preface to the detailed Requirements and Security Assessment Procedures:

1. **Description of Scope of Review**
   - Describe scope of review coverage, per the Scope of PA-DSS section above
   - Timeframe of validation
   - PA-DSS version used for the assessment
   - List of documentation reviewed
2. **Executive Summary**

   Include the following:
   - Product Name
   - Product Version and related platforms covered
   - List of resellers and/or integrators for this product
   - Operating system(s) with which the payment application was tested
   - Database software used or supported by the payment application
   - Brief description of the payment application/family of products (2-3 sentences)
   - 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:
     - Connections into and out of a customer's network
     - Components within the customer's network, including POS devices, systems, databases, and web servers as applicable
     - Other necessary payment application/components, as applicable
   - 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)
   - A dataflow diagram that shows all flows of cardholder data, including authorization, capture, settlement, and chargeback flows as applicable

Copyright 2010 PCI Security Standards Council LLC

- 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.):
  - List of all elements of stored cardholder data
  - How data store is secured
  - How access to data store is logged
- List all payment application related software components, including third-party software requirements and dependencies
- Description of payment application's end to end authentication methods, including application authentication mechanism, authentication database, and security of data storage
- Description of role of payment application in a typical implementation and what other types of payment applications are necessary for a full payment implementation
- 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).
- 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.

Note: Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment *must also be completed and submitted with the completed PA-DSS report.*

3. Findings and Observations

- All PA-QSAs must use the following template to provide detailed report descriptions and findings
- Describe tests performed other than those included in the testing procedures column.
- 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.

4. Contact Information and Report Date

- Software vendor contact information (include URL, phone number, and e-mail address)
- PA-QSA contact information (include name, phone number and e-mail address)
- PA-QSA Quality Assurance (QA) primary contact information (include primary QA contact's name, phone number and e-mail address)
- Date of report

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Completion Steps

This document contains the Requirements and Security Assessment Procedures table, as well as *Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment*. The Requirements and Security Assessment Procedures detail the procedures that must be performed by the PA-QSA. The *Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment* must be completed by the PA-QSA to confirm the status and capabilities of the testing laboratory used to conduct this PA-DSS assessment.

The PA-QSA must perform the following steps:

1. Complete the Report on Validation using this document as a template:
   a. Complete the preface for the Report on Validation, in accordance with the section entitled "Instructions and Content for Report on Validation"
   b. Complete and document all steps detailed in the Requirements and Security Assessment Procedures, including brief descriptions of controls observed in the "In Place" column, and noting any comments. *Please note that a report with any "Not in Place" opinions should not be submitted to PCI SSC until all items are noted as "In Place."*
2. Complete *Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment.*
3. Complete and sign *an Attestation of Validation* (both PA-QSA and software vendor). The Attestation of Validation is available on the PCI SSC website (www.pcisecuritystandards.org).
4. After completion, submit all of the above documents to PCI SSC according to the *PA-DSS Program Guide.*

PA-DSS Program Guide

Please refer to the *PA-DSS Program Guide* for information about PA-DSS program management, including the following topics:

- PA-DSS report submission and acceptance processes
- Annual renewal process for payment applications included on the List of PA-DSS Validated Applications
- Transition of PABP-validated applications to the List of PA-DSS Validated Payment Applications
- Notification responsibilities in the event a listed payment application is determined to be at fault in a compromise.

PCI SSC reserves the right to require revalidation due to significant changes to the Payment Application Data Security Standard and/or due to specifically identified vulnerabilities in a listed payment application.

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements and Security Assessment Procedures

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1. Do not retain full magnetic stripe, card verification 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.			
	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.			
	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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.)[3] 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			
1.1.2 After authorization, do not store the card verification 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 verification 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			

[3] 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.

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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			
1.1.4 Securely delete any magnetic stripe data, card verification 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 verification 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			
	1.1.4.b Verify the vendor provides a secure wipe tool or procedure 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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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 verification 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			
	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.			
	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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.			
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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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. ***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** 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			
	2.3.b Examine several tables or files from data repositories created or generated by the application to verify the 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.			
	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.			
	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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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).			
	2.4.b Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).			
	2.4.c If the application creates or generates files on removable media, verify that cardholder data on removable media is 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-encrypting keys used to protect data-encrypting keys—such key-encrypting 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.			
	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			
	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			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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			
	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.			
2.6.2 Secure cryptographic key distribution	**2.6.2** Verify that key-management procedures are implemented 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.			
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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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-encrypting 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.			
	2.6.5.b Verify that key-management procedures are implemented 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.			
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.			
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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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-encrypting key (KEK) provided that residual data-encrypting 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			
	2.7.b Verify vendor provides a tool or procedure to render 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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.			
	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).			
	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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
	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.)			
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.			
	3.1.1.b For subsequent changes after installation.			
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.			
	3.1.2.b For subsequent changes after installation.			
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			
	3.1.3.b For subsequent changes after installation.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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			
	3.1.4.b For subsequent changes after installation			
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			
	3.1.5.b For subsequent changes after installation			
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.			
	3.1.6.a By completion of the installation process			
	3.1.6.b For subsequent changes after installation			
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			
	3.1.7.b For subsequent changes after installation			
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			
	3.1.8.b For subsequent changes after installation			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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			
	3.1.9.b For subsequent changes after installation			
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			
	3.1.10.b For subsequent changes after installation			
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.			
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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.			
	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.			
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.			
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.			
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.			
4.2.4 Invalid logical access attempts	**4.2.4** Verify invalid logical access attempts are logged.			
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.			
4.2.6 Initialization of the application audit logs	**4.2.6** Verify initialization of application audit logs is logged.			
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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.			
4.3.2 Type of event	**4.3.2** Verify type of event is included in log entries.			
4.3.3 Date and time	**4.3.3** Verify date and time stamp is included in log entries.			
4.3.4 Success or failure indication	**4.3.4** Verify success or failure indication is included in log entries.			
4.3.5 Origination of event	**4.3.5** Verify origination of event is included in 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.			
4.4. Payment application must facilitate centralized logging. ***Note:*** *Examples of this functionality may include, but are not limited to:* ▪ 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.a** Validate that payment application provides functionality that facilitates a merchant's ability to assimilate logs into their centralized log server.			
	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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.			
	5.1.b Verify 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.			
	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.			
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.			
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.			
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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.			
	5.2.b Interview a sample of developers and obtain evidence that 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:			
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.)			
5.2.2 Buffer Overflow	**5.2.2** Buffer Overflow (Validate buffer boundaries and truncate input strings.)			
5.2.3 Insecure cryptographic storage	**5.2.3** Insecure cryptographic storage (Prevent cryptographic flaws.)			
5.2.4 Insecure communications	**5.2.4** Insecure communications (Properly encrypt all authenticated and sensitive communications.)			
5.2.5 Improper error handling	**5.2.5** Improper error handling (Do not leak information via error messages)			
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			
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.)			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.)			
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.)			
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.			
	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:			
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.			
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.			
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			
	5.3.3.b Verify that all changes (including patches) are tested for compliance with 5.2 before being released.			
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.			
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).	**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"			
	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".			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
Aligns with PCI DSS Requirement 2.2.2	**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.			
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:			
	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			
	6.1.b Verify default SNMP community strings on wireless devices were changed			
	6.1.c Verify default passwords/passphrases on access points were changed			
	6.1.d Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks			
	6.1.e Verify other security-related wireless vendor defaults were changed, if applicable			
	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			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.	**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.			
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.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).			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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".)			
	7.1.b Verify the processes to identify new security vulnerabilities include using outside sources for security vulnerability information			
	7.1.c Verify that processes include testing of payment applications for new vulnerabilities			
	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).			
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			
	7.2.b Review processes to verify that patches and updates are delivered in a secure manner 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			
	7.2.d Review processes to verify that patches and updates are integrity tested 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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.			
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).			
	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).			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.			
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).			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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 3.1.10)* ▪ *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 Requirement3.1.8)* ▪ *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.			
	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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.			
	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.			
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.			
	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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.			
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).			
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.			
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.			
	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.			
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.			

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
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.			
	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.			
	13.2.1.b Select a sample of resellers and integrators and interview them to verify they received the training materials.			

Copyright 2010 PCI Security Standards Council LLC

Appendix A: Summary of Contents for the *PA-DSS Implementation Guide*

The intent of this Appendix is to summarize those PA-DSS requirements that have related *PA-DSS Implementation Guide* topics, to explain the content for the *PA-DSS Implementation Guide,* and to spell out responsibilities for implementing the related controls.

PA-DSS Requirement	PA-DSS Topic	Implementation Guide Content	Control Implementation Responsibility
1.1.4	Delete sensitive authentication data stored by previous payment application versions.	▪ Historical data must be removed (magnetic stripe data, card verification codes, PINs, or PIN blocks stored by previous versions of the payment application) ▪ How to remove historical data ▪ Such removal is absolutely necessary for PCI DSS compliance	**Software Vendor**: Provide tool or procedure for customers to securely remove data stored by previous versions, per PA-DSS Requirement 1.1.4. **Customers & Resellers/Integrators**: Delete any historical data per the *PA-DSS Implementation Guide* and PA-DSS Requirement 1.1.4.
1.1.5	Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.	▪ Sensitive authentication data (pre-authorization) must only be collected when needed to solve a specific problem ▪ Such data must be stored only in specific, known locations with limited access ▪ Only collect a limited amount of such data as needed to solve a specific problem ▪ Sensitive authentication data must be encrypted while stored ▪ Such data must be securely deleted immediately after use	**Software Vendor**: Perform any troubleshooting of customer's problems according to PA-DSS Requirement 1.1.5.a. **Customers & Resellers/Integrators:** Troubleshoot any problems per the *PA-DSS Implementation Guide* and PA-DSS Requirement 1.1.5.a.
2.1	Purge cardholder data after customer-defined retention period.	▪ Cardholder data must be purged after it exceeds the customer-defined retention period ▪ All locations where payment application stores cardholder data	**Software Vendor**: Provide guidance to customers that cardholder data exceeding customer-defined retention periods must be purged and where such data is stored by the payment application. **Customers & Resellers/Integrators**: Purge cardholder data exceeding customer-defined retention period.

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirement	PA-DSS Topic	Implementation Guide Content	Control Implementation Responsibility
2.5	Protect keys used to secure cardholder data against disclosure and misuse.	▪ Restrict access to keys to the fewest number of custodians necessary. ▪ Store keys securely in the fewest possible locations and forms	**Software Vendor**: Provide guidance to customers that keys used to secure cardholder data should be stored securely in the fewest possible locations, and access to keys must be restricted to the fewest possible custodians. **Customers & Resellers/Integrators**: Store keys securely in the fewest possible locations, and restrict access to keys to the fewest possible custodians.
2.6	Implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.	▪ 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 PA-DSS requirements 2.6.1 through 2.6.7.	**Software Vendor**: Provide instructions to customers that access cryptographic keys used for encryption of cardholder data to implement key management processes and procedures. **Customers & Resellers/Integrators**: Implement key management processes and procedures for cryptographic keys used for encryption of cardholder data per *PA-DSS Implementation Guide* and PA-DSS Requirement 2.6.
2.7	Render irretrievable cryptographic key material or cryptograms stored by previous payment application versions.	▪ Cryptographic material must be rendered irretrievable ▪ How to render cryptographic material irretrievable ▪ Such irretrievability is absolutely necessary for PCI compliance ▪ How to re-encrypt historic data with new keys	**Software Vendor**: Provide tool or procedure to securely remove cryptographic key material or cryptograms stored by previous versions, per PA-DSS Requirement 1.1.5, provide tool or procedure to re-encrypt historic data with new keys. **Customers & Resellers/Integrators**: Delete any historical cryptographic material per *PA-DSS Implementation Guide* and PA-DSS Requirement 1.1.5.

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirement	PA-DSS Topic	Implementation Guide Content	Control Implementation Responsibility
3.1	Use unique user IDs and secure authentication for administrative access and access to cardholder data.	▪ That the payment application enforces secure authentication for any authentication credentials (e.g. users, passwords) that the application generates by: – Enforcing secure changes to authentication credentials by the completion of installation and for any subsequent changes (after installation) per PA-DSS requirements 3.1.1 through 3.1. ▪ Assign secure authentication to default accounts (even if not used), and disable or do not use the accounts. ▪ How to change and create authentication credentials when such credentials are not generated or managed by the payment application, per PCI DSS Requirements 8.5.8 through 8.5.15, by the completion of installation and for subsequent changes after installation, for all application level accounts with administrative access or access to cardholder data.	**Software Vendor**: When the payment application generates or manages authentication credentials, ensure payment application enforces customer's use of unique user IDs and secure authentication for payment application accounts/passwords, per PA-DSS Requirements 3.1.1 through 3.1.10. When authentication credentials are not generated or managed by the payment application, ensure the *PA-DSS Implementation Guide* provides clear and unambiguous guidance for customers and resellers/integrators on how to change and create secure authentication credentials per PA-DSS Requirements 3.1.1 through 3.1.10. **Customers & Resellers/Integrators**: Establish and maintain unique user IDs and secure authentication per the *PA-DSS Implementation Guide* and PA-DSS Requirements 3.1.1 through 3.1.10.
3.2	Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.	Use unique user names and secure authentication to access any PCs, servers, and databases with payment applications and/or cardholder data, PA-DSS requirements 3.1.1 through 3.1.10.	**Software Vendor**: Ensure payment application supports customer's use of unique user IDs and secure authentication for accounts/passwords if set by vendor to access PCs, servers, and databases, per PA-DSS requirements 3.1.2 through 3.1.9. **Customers & Resellers/Integrators**: Establish and maintain unique user IDs and secure authentication per the *PA-DSS Implementation Guide* and PA-DSS requirements 3.1.2 through 3.1.10.
4.1	Implement automated audit trails.	▪ Set PCI DSS-compliant log settings, per PA-DSS Requirements 4.2, 4.3 and 4.4 ▪ Logs must be enabled, and disabling the logs will result in non-compliance with PCI DSS.	**Software Vendor**: Ensure payment application supports customer's use of compliant logs per PA-DSS Requirements 4.2, 4.3 and 4.4. **Customers & Resellers/Integrators:** Establish and maintain PCI DSS-compliant logs per the *PA-DSS Implementation Guide* and PA-DSS Requirements 4.2, 4.3 and 4.4.

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirement	PA-DSS Topic	Implementation Guide Content	Control Implementation Responsibility
4.4	Facilitate centralized logging.	Provide instructions and procedures for incorporating the payment application logs into a centralized logging server.	**Software Vendor**: Ensure payment application supports centralized logging in customer environments per PA-DSS Requirement 4.4. **Customers & Resellers/Integrators:** Establish and maintain centralized logging per the *PA-DSS Implementation Guide* and PA-DSS Requirement 4.4.
5.4	Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.	Document all required protocols, services, components, and dependent software and hardware that are necessary for any functionality of the payment application.	**Software Vendor:** Ensure payment application supports customer's use of only necessary and secure protocols, services, etc., by 1) having only necessary protocols, services, etc., established "out of the box" by default, 2) having those necessary protocols, services, etc., securely configured by default, and 3) by documenting necessary protocols, services, etc., as a reference for customers and resellers/integrators. **Customers and Resellers/Integrators:** Use the documented list from the *Implementation Guide* to ensure only necessary and secure protocols, services, etc., are used on the system, in accordance with PA-DSS Requirement 5.4.
6.1	Securely implement wireless technology.	If wireless is used within payment environment: ▪ Change wireless vendor defaults, including default wireless encryption keys, passwords, and SNMP community strings ▪ Install a firewall: – Between any wireless networks and systems that store cardholder data, and – Configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment	**Software Vendor**: Instruct customers and resellers/integrators, that if wireless technology is used with the payment application, that wireless vendor default settings must be changed per PA-DSS Requirement 6.1. **Customers & Resellers/Integrators**: For wireless implemented into the payment environment by customers or resellers/integrators, change vendor defaults per PA-DSS Requirement 6.1 and install a firewall per the *PA-DSS Implementation Guide* and PCI DSS Requirement 2.1.1.

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirement	PA-DSS Topic	Implementation Guide Content	Control Implementation Responsibility
6.2	Secure transmissions of cardholder data over wireless networks.	If payment application is implemented into a wireless environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission of cardholder data.	**Software Vendor**: Instruct customers and resellers/integrators, that if wireless technology is used with the payment application, that secure encrypted transmissions must be implemented, per PA-DSS Requirement 6.2. **Customers & Resellers/Integrators**: For wireless implemented into the payment environment by customers or resellers/integrators, use secure encrypted transmissions per the *PA-DSS Implementation Guide* and PA-DSS Requirement 6.2.
9.1	Store cardholder data only on servers not connected to the Internet.	Do not store cardholder data on Internet-accessible systems (for example, web server and database server must not be on same server).	**Software Vendor**: Ensure payment application does not require data storage in the DMZ or on Internet-accessible systems, and will allow use of a DMZ per PA-DSS Requirement 9. **Customers & Resellers/Integrators**: Establish and maintain payment applications so that cardholder data is not stored on Internet-accessible systems, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 9
10.2	Implement two-factor authentication for remote access to payment application.	Use two-factor authentication (user ID and password and an additional authentication item such as a token) if the payment application may be accessed remotely.	**Software Vendor**: Ensure payment application supports customers' use of two-factor authentication, per PA-DSS Requirement 10.2. **Customers & Resellers/Integrators**: Establish and maintain two-factor authentication for remote access to payment application, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 10.2.
10.3.1	Securely deliver remote payment application updates.	▪ Activate remote-access technologies for payment application updates only when needed for downloads, and turn off immediately after download completes, per PCI DSS Requirement 12.3.9. ▪ If computer is connected via VPN or other high-speed connection, receive remote payment application updates via a securely configured firewall or personal firewall per PCI DSS Requirement 1.	**Software Vendor**: Deliver remote payment application updates securely per PA-DSS 10.3 **Customers & Resellers/Integrators**: Receive remote payment application updates from vendor securely, per the *PA-DSS Implementation Guide,* PA-DSS Requirement 10.3 and PCI DSS Requirement 1.

Copyright 2010 PCI Security Standards Council LLC

PA-DSS Requirement	PA-DSS Topic	Implementation Guide Content	Control Implementation Responsibility
10.3.2	Securely implement remote access software.	Implement and use remote access software security features if remote access software is used to remotely access the payment application or payment environment.	**Software Vendor**: (1) If vendor uses remote access products to access customer sites, use remote access security features such as those specified in PA-DSS Requirement **10.3.2**. (2) Ensure payment application supports customers' use of remote access security features. **Customers & Resellers/Integrators**: Use remote access security features if you allow remote access to payment applications, per the *PA-DSS Implementation Guide* and PA-DSS Requirement **10.3.2**.
11.1	Secure transmissions of cardholder data over public networks.	Implement and use strong cryptography and security protocols for secure cardholder data transmission over public networks.	**Software Vendor**: Ensure payment application supports customer's use of strong cryptography and security protocols for transmissions of cardholder data over public networks, per PA-DSS Requirement 11.1. **Customers & Resellers/Integrators**: Establish and maintain strong cryptography and security protocols for transmissions of cardholder data, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 11.1.
11.2	Encrypt cardholder data sent over end-user messaging technologies.	Implement and use a solution that renders the PAN unreadable or implements strong cryptography if PANs can be sent with end-user messaging technologies.	**Software Vendor**: Ensure payment application supports the encryption or rendering unreadable of PANs if sent with end-user messaging technologies, per PA-DSS Requirement 11.2. **Customers & Resellers/Integrators**: Encrypt all PANs sent with end-user messaging technologies, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 11.2.
12.1	Encrypt non-console administrative access.	Implement and use strong cryptography (such as SSH, VPN, or SSL/TLS) for encryption of any non-console administrative access to payment application or servers in cardholder data environment.	**Software Vendor**: Ensure payment application supports customer's encryption of any non-console administrative access, per PA-DSS Requirement 12.1. **Customers & Resellers/Integrators**: Encrypt all non-console administrative access, per the *PA-DSS Implementation Guide* and PA-DSS Requirement 12.1

Copyright 2010 PCI Security Standards Council LLC

Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment

For: *Software Vendor Application Name Version Number*

For each PA-DSS assessment conducted, the PA-QSA must complete this document to confirm the status and capabilities of the laboratory used to conduct the testing for the PA-DSS assessment. This completed document must be submitted along with the completed *PA-DSS Requirements and Security Assessment Procedures* document.

For each Laboratory Validation Procedure, indicate (by using columns titled "Completed in PA-QSA's Lab" or "Completed in Vendor's Lab") whether laboratory used for the assessment and the laboratory undergoing these validation procedures was the PA-QSA's laboratory or software vendor's laboratory.

Describe laboratory testing architecture and environment in place for this PA-DSS review:

Describe how the real-world use of the payment application was simulated in the laboratory for this PA-DSS review:

Laboratory Requirement	Laboratory Validation Procedure	Completed in		Comments
		PA-QSA's Lab	Vendor's Lab	
1. Install payment application per vendor's installation instructions or training provided to customer.	**1.** Verify that the vendor's installation manual or training provided to customers was used to perform the default installation for the payment application product on all platforms listed in the PA-DSS report.	☐	☐	
2. Install and test all payment application versions listed in PA-DSS report.	**2.a** Verify that all common implementations (including region/country specific versions) of the payment application to be tested were installed.	☐	☐	
	2.b Verify that all payment application versions and platforms were tested.	☐	☐	
	2.c Verify that all critical payment application functionalities were tested.	☐	☐	

Copyright 2010 PCI Security Standards Council LLC

Laboratory Requirement	Laboratory Validation Procedure	Completed in		Comments
		PA-QSA's Lab	Vendor's Lab	
3. Install and implement all PCI DSS required security devices.	**3.** Verify that all security devices required by PCI DSS (for example, firewalls and anti-virus software) were implemented on test systems.	☐	☐	
4. Install and/or configure all PCI DSS required security settings.	**4.** Verify all PCI DSS-compliant system settings, patches, etc., were implemented on test systems for operating systems, system software, and applications used by the payment application.	☐	☐	
5. Simulate real-world use of the payment application.	**5.a** The laboratory simulates the 'real world' use of the payment application, including all systems and applications where the payment application is implemented. For example, a standard implementation of a payment application might include a client/server environment within a retail storefront with a POS machine, and back office or corporate network. The laboratory simulates the total implementation.	☐	☐	
	5.b The laboratory uses only test card numbers for the simulation/testing – live PANs are not used for testing. ***Note:*** *Test cards can usually be obtained from the vendor or a processor or acquirer.*	☐	☐	
	5.c The laboratory runs the payment application's authorization and/or settlement functions and all output is examined per item 6 below.	☐	☐	
	5.d The laboratory and/or processes map all output produced by the payment application for every possible scenario, whether temporary, permanent, error processing, debugging mode, log files, etc.	☐	☐	
	5.e The laboratory and/or processes simulate and validate all functions of the payment application, to include generation of all error conditions and log entries using both simulated 'live' data and invalid data.	☐	☐	

Copyright 2010 PCI Security Standards Council LLC

Laboratory Requirement	Laboratory Validation Procedure	Completed in		Comments
		PA-QSA's Lab	Vendor's Lab	
6. Provide capabilities for, and test using, the following penetration testing methodologies:	**6.a Use of forensic tools/methods:** Forensic tools/methods were used to search all identified output for evidence of sensitive authentication data (commercial tools, scripts, etc.), per PA-DSS Requirement 1.1.1–1.1.3.[4]	☐	☐	
	6.b Attempt to exploit application vulnerabilities: Current vulnerabilities (for example, the OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, etc.), were used to attempt to exploit the payment application(s), per PA-DSS Requirement 5.2.	☐	☐	
	6.c Laboratory and/or processes attempted to execute arbitrary code during the payment application update process: Run the update process with arbitrary code per PA-DSS Requirement 7.2.b.	☐	☐	
7. Use vendor's lab ONLY after verifying all requirements are met.	**7.a** If use of the software vendor's lab is necessary (for example, the PA-QSA does not have the mainframe, AS400, or Tandem the payment application runs on), the PA-QSA can either (1) use equipment on loan from the Vendor or (2) use the vendor's lab facilities, provided that this is detailed in the report together with the location of the tests. For either option, the PA-QSA verified that the vendor's equipment and lab meet the following requirements:	☐	☐	
	7.b The PA-QSA verifies that the vendor's lab meets all above requirements specified in this document and documents the details in the report.	☐	☐	
	7.c The PA-QSA must validate the clean installation of the remote lab environment to ensure the environment truly simulates a real world situation and that the vendor has not modified or tampered with the environment in any way.	☐	☐	

[4] 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.

Copyright 2010 PCI Security Standards Council LLC

Laboratory Requirement	Laboratory Validation Procedure	Completed in		Comments
		PA-QSA's Lab	Vendor's Lab	
	7.d All testing is executed by the PA-QSA (the vendor cannot run tests against their own application).	☐	☐	
	7.e All testing is either (1) performed while onsite at the vendor's premises, or (2) performed remotely via a network connection using a secure link (for example, VPN).	☐	☐	
	7.f Use only test card numbers for the simulation/testing—do not use live PANs for testing. These test cards can usually be obtained from the vendor or a processor or acquirer.	☐	☐	
8. Maintain an effective quality assurance (QA) process	**8.a** PA-QSA QA personnel verify that all platforms identified in the PA-DSS report were included in testing.	☐	☐	
	8.b PA-QSA QA personnel verify that all PA-DSS requirements were tested against.	☐	☐	
	8.c The PA-QSA QA personnel verify that PA-QSA laboratory configurations and processes meet requirements and were accurately documented in the report.	☐	☐	
	8.d PA-QSA QA personnel verify that the report accurately presents the results of testing.	☐	☐	

Copyright 2010 PCI Security Standards Council LLC