Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire D and Attestation of Compliance for Merchants

All other SAQ-Eligible Merchants

Version 3.0

February 2014

Document Changes

Date	Version	Description
October 2008	1.2	To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 2010	2.0	To align content with new PCI DSS v2.0 requirements and testing procedures.
February 2014	3.0	To align content with PCI DSS v3.0 requirements and testing procedures and incorporate additional response options.

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Table of Contents

Document Changes i

Before You Begin iii

PCI DSS Self-Assessment Completion Steps iii

Understanding the Self-Assessment Questionnaire iii

Expected Testing iv

Completing the Self-Assessment Questionnaire iv

Guidance for Non-Applicability of Certain, Specific Requirements v

Understanding the difference between Not Applicable and Not Tested v

Legal Exception v

Section 1: Assessment Information 1

Section 2: Self-Assessment Questionnaire D for Merchants 4

Build and Maintain a Secure Network and Systems 4

Requirement 1: Install and maintain a firewall configuration to protect data 4

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters 9

Protect Cardholder Data 14

Requirement 3: Protect stored cardholder data 14

Requirement 4: Encrypt transmission of cardholder data across open, public networks 22

Maintain a Vulnerability Management Program 24

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs 24

Requirement 6: Develop and maintain secure systems and applications 26

Implement Strong Access Control Measures 34

Requirement 7: Restrict access to cardholder data by business need to know 34

Requirement 8: Identify and authenticate access to system components 36

Requirement 9: Restrict physical access to cardholder data 42

Regularly Monitor and Test Networks 50

Requirement 10: Track and monitor all access to network resources and cardholder data 50

Requirement 11: Regularly test security systems and processes 56

Maintain an Information Security Policy 63

Requirement 12: Maintain a policy that addresses information security for all personnel 63

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers 70

Appendix B: Compensating Controls Worksheet 71

Appendix C: Explanation of Non-Applicability 72

Appendix D: Explanation of Requirements Not Tested 73

Section 3: Validation and Attestation Details 74

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Before You Begin

SAQ D for Merchants applies to SAQ-eligible merchants not meeting the criteria for any other SAQ type. Examples of merchant environments that would use SAQ D may include but are not limited to:

- E-commerce merchants who accept cardholder data on their website.
- Merchants with electronic storage of cardholder data
- Merchants that don't store cardholder data electronically but that do not meet the criteria of another SAQ type
- Merchants with environments that might meet the criteria of another SAQ type, but that have additional PCI DSS requirements applicable to their environment

While many organizations completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some requirements do not apply. See the guidance below for information about the exclusion of certain, specific requirements.

PCI DSS Self-Assessment Completion Steps

1. Identify the applicable SAQ for your environment – refer to the *Self-Assessment Questionnaire Instructions and Guidelines* document on PCI SSC website for information.
2. Confirm that your environment is properly scoped and meets the eligibility criteria for the SAQ you are using.
3. Assess your environment for compliance with PCI DSS requirements.
4. Complete all sections of this document:
   - Section 1 (Part 1 & 2 of the AOC) – Assessment Information and Executive Summary.
   - Section 2 – PCI DSS Self-Assessment Questionnaire (SAQ D)
   - Section 3 (Parts 3 & 4 of the AOC) – Validation and Attestation Details and Action Plan for Non-Compliant Requirements (if applicable)
5. Submit the SAQ and Attestation of Compliance, along with any other requested documentation—such as ASV scan reports—to your acquirer, payment brand or other requester.

Understanding the Self-Assessment Questionnaire

The questions contained in the "PCI DSS Question" column in this self-assessment questionnaire are based on the requirements in the PCI DSS.

Additional resources that provide guidance on PCI DSS requirements and how to complete the self-assessment questionnaire have been provided to assist with the assessment process. An overview of some of these resources is provided below:

Document	Includes:
PCI DSS *(PCI Data Security Standard Requirements and Security Assessment Procedures)*	• Guidance on Scoping • Guidance on the intent of all PCI DSS Requirements • Details of testing procedures • Guidance on Compensating Controls
SAQ Instructions and Guidelines documents	• Information about all SAQs and their eligibility criteria • How to determine which SAQ is right for your organization

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms	• Descriptions and definitions of terms used in the PCI DSS and self-assessment questionnaires

These and other resources can be found on the PCI SSC website *(www.pcisecuritystandards.org)*. Organizations are encouraged to review the PCI DSS and other supporting documents before beginning an assessment.

Expected Testing

The instructions provided in the "Expected Testing" column are based on the testing procedures in the PCI DSS, and provide a high-level description of the types of testing activities that should be performed in order to verify that a requirement has been met. Full details of testing procedures for each requirement can be found in the PCI DSS.

Completing the Self-Assessment Questionnaire

For each question, there is a choice of responses to indicate your company's status regarding that requirement. ***Only one response should be selected for each question.***

A description of the meaning for each response is provided in the table below:

Response	When to use this response:
Yes	The expected testing has been performed, and all elements of the requirement have been met as stated.
Yes with CCW (Compensating Control Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Control Worksheet (CCW) in Appendix B of the SAQ. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in the PCI DSS.
No	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
N/A (Not Applicable)	The requirement does not apply to the organization's environment. (See *Guidance for Non-Applicability of Certain, Specific Requirements* below for examples.) All responses in this column require a supporting explanation in Appendix C of the SAQ.
Not Tested	The requirement was not included for consideration in the assessment, and was not tested in any way. (See *Understanding the difference between Not Applicable and Not Tested* below for examples of when this option should be used.) All responses in this column require a supporting explanation in Appendix D of the SAQ.

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Guidance for Non-Applicability of Certain, Specific Requirements

While many organizations completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some requirements do not apply. For example, a company that does not use wireless technology in any capacity would not be expected to validate compliance with the sections of the PCI DSS that are specific to managing wireless technology. Similarly, an organization that does not store any cardholder data electronically at any time would not need to validate requirements related to secure storage of cardholder data (for example, Requirement 3.4).

Examples of requirements with specific applicability include:

- The questions specific to securing wireless technologies (for example, Requirements 1.2.3, 2.1.1, and 4.1.1) only need to be answered if wireless is present anywhere in your network. Note that Requirement 11.1 (use of processes to identify unauthorized wireless access points) must still be answered even if you don't use wireless technologies in your network, since the process detects any rogue or unauthorized devices that may have been added without your knowledge.
- The questions specific to application development and secure coding (Requirements 6.3 and 6.5) only need to be answered if your organization develops its own custom applications.
- The questions for Requirements 9.1.1 and 9.3 only need to be answered for facilities with "sensitive areas" as defined here: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store, but does include retail store back-office server rooms that store cardholder data, and storage areas for large quantities of cardholder data.

If any requirements are deemed not applicable to your environment, select the "N/A" option for that specific requirement, and complete the "Explanation of Non-Applicability" worksheet in Appendix C for each "N/A" entry.

Understanding the difference between Not Applicable and Not Tested

Requirements that are deemed to be not applicable to an environment must be verified as such. Using the wireless example above, for an organization to select "N/A" for Requirements 1.2.3, 2.1.1, and 4.1.1, the organization would first need to confirm that there are no wireless technologies used in their CDE or that connect to their CDE. Once this has been confirmed, the organization may select "N/A" for those specific requirements.

If a requirement is completely excluded from review without any consideration as to whether it *could* apply, the "Not Tested" option should be selected. Examples of situations where this could occur may include:

- An organization may be asked by their acquirer to validate a subset of requirements—for example: using the prioritized approach to validate certain milestones.
- An organization may wish to validate a new security control that impacts only a subset of requirements—for example, implementation of a new encryption methodology that requires assessment of PCI DSS Requirements 2, 3 and 4.
- A service provider organization might offer a service which covers only a limited number of PCI DSS requirements—for example, a physical storage provider may only wish to validate the physical security controls per PCI DSS Requirement 9 for their storage facility.

In these scenarios, the organization only wishes to validate certain PCI DSS requirements even though other requirements might also apply to their environment.

Legal Exception

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS requirement, check the "No" column for that requirement and complete the relevant attestation in Part 3.

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact acquirer (merchant bank) or the payment brands to determine reporting and submission procedures.

Part 1. Merchant and Qualified Security Assessor Information					
Part 1a. Merchant Organization Information					
Company Name:			DBA (doing business as):		
Contact Name:			Title:		
ISA Name(s) (if applicable):			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Zip:	
URL:					
Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:					
Lead QSA Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Zip:	
URL:					

Part 2. Executive Summary		
Part 2a. Type of Merchant Business (check all that apply)		
☐ Retailer	☐ Telecommunication	☐ Grocery and Supermarkets
☐ Petroleum	☐ E-Commerce	☐ Mail order/telephone order (MOTO)
☐ Others (please specify):		

What types of payment channels does your business serve?	Which payment channels are covered by this SAQ?
☐ Mail order/telephone order (MOTO)	☐ Mail order/telephone order (MOTO)
☐ E-Commerce	☐ E-Commerce
☐ Card-present (face-to-face)	☐ Card-present (face-to-face)

Note: *If your organization has a payment channel or process that is not covered by this SAQ, consult your acquirer or payment brand about validation for the other channels.*

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?	

Part 2c. Locations

List types of facilities and a summary of locations included in the PCI DSS review (for example, retail outlets, corporate offices, data centers, call centers, etc.)

Type of facility	Location(s) of facility (city, country)

Part 2d. Payment Application

Does the organization use one or more Payment Applications? ☐ Yes ☐ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Chase Mobile Checkout		Chase Paymentech	☐ Yes ☒ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	The cardholder environment consists of Chase Mobile Swipe Devices and tablets. The CDE utilizes the Chase Mobile Checkout Application.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2f. Third-Party Service Providers	
Does your company share cardholder data with any third-party service providers (for example, gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?	☐ Yes ☒ No
If Yes:	

Name of service provider:	Description of services provided:

Note: *Requirement 12.8 applies to all entities in this list.*

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Section 2: Self-Assessment Questionnaire D for Merchants

Note: *The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the* PCI DSS Requirements and Security Assessment Procedures *document.*

Self-assessment completion date:

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect data

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
1.1	Are firewall and router configuration standards established and implemented to include the following:						
1.1.1	Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations?	▪ Review documented process ▪ Interview personnel ▪ Examine network configurations	☐	☐	☐	☒	☐
1.1.2	(a) Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?	▪ Review current network diagram ▪ Examine network configurations	☐	☐	☐	☒	☐
	(b) Is there a process to ensure the diagram is kept current?	▪ Interview responsible personnel	☐	☐	☐	☒	☐
1.1.3	(a) Is there a current diagram that shows all cardholder data flows across systems and networks?	▪ Review current dataflow diagram ▪ Examine network configurations.	☐	☐	☐	☒	☐
	(b) Is there a process to ensure the diagram is kept current?	▪ Interview personnel	☐	☐	☐	☒	☐
1.1.4	(a) Is a firewall required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?	▪ Review firewall configuration standards ▪ Observe network configurations to verify that a firewall(s) is in place	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
	(b) Is the current network diagram consistent with the firewall configuration standards?	▪ Compare firewall configuration standards to current network diagram	☐	☐	☐	☒	☐
1.1.5	Are groups, roles, and responsibilities for logical management of network components assigned and documented in the firewall and router configuration standards?	▪ Review firewall and router configuration standards ▪ Interview personnel	☐	☐	☐	☒	☐
1.1.6	(a) Do firewall and router configuration standards include a documented list of services, protocols, and ports, including business justification (for example, hypertext transfer protocol (HTTP), Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols)?	▪ Review firewall and router configuration standards	☐	☐	☐	☒	☐
	(b) Are all insecure services, protocols, and ports identified, and are security features documented and implemented for each identified service? ***Note:*** *Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.*	▪ Review firewall and router configuration standards ▪ Examine firewall and router configurations	☐	☐	☐	☒	☐
1.1.7	(a) Do firewall and router configuration standards require review of firewall and router rule sets at least every six months?	▪ Review firewall and router configuration standards	☐	☐	☐	☒	☐
	(b) Are firewall and router rule sets reviewed at least every six months?	▪ Examine documentation from firewall reviews	☐	☐	☐	☒	☐
1.2	Do firewall and router configurations restrict connections between untrusted networks and any system in the cardholder data environment as follows: ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*						

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
1.2.1	(a) Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment?	▪ Review firewall and router configuration standards ▪ Examine firewall and router configurations	☐	☐	☐	☒	☐
	(b) Is all other inbound and outbound traffic specifically denied (for example by using an explicit "deny all" or an implicit deny after allow statement)?	▪ Review firewall and router configuration standards ▪ Examine firewall and router configurations	☐	☐	☐	☒	☐
1.2.2	Are router configuration files secured from unauthorized access and synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted)?	▪ Review firewall and router configuration standards ▪ Examine router configuration files and router configurations	☐	☐	☐	☒	☐
1.2.3	Are perimeter firewalls installed between all wireless networks and the cardholder data environment, and are these firewalls configured to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment?	▪ Review firewall and router configuration standards ▪ Examine firewall and router configurations	☐	☐	☐	☒	☐
1.3	Is direct public access prohibited between the Internet and any system component in the cardholder data environment, as follows:						
1.3.1	Is a DMZ implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports?	▪ Examine firewall and router configurations	☐	☐	☐	☒	☐
1.3.2	Is inbound Internet traffic limited to IP addresses within the DMZ?	▪ Examine firewall and router configurations	☐	☐	☐	☒	☐
1.3.3	Are direct connections prohibited for inbound or outbound traffic between the Internet and the cardholder data environment?	▪ Examine firewall and router configurations	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
1.3.4	Are anti-spoofing measures implemented to detect and block forged sourced IP addresses from entering the network? (For example, block traffic originating from the internet with an internal address.)	▪ Examine firewall and router configurations	☐	☐	☐	☒	☐
1.3.5	Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?	▪ Examine firewall and router configurations	☐	☐	☐	☒	☐
1.3.6	Is stateful inspection, also known as dynamic packet filtering, implemented—that is, only established connections are allowed into the network?	▪ Examine firewall and router configurations	☐	☐	☐	☒	☐
1.3.7	Are system components that store cardholder data (such as a database) placed in an internal network zone, segregated from the DMZ and other untrusted networks?	▪ Examine firewall and router configurations	☐	☐	☐	☒	☐
1.3.8	(a) Are methods in place to prevent the disclosure of private IP addresses and routing information to the Internet? ***Note:*** *Methods to obscure IP addressing may include, but are not limited to:* • Network Address Translation (NAT) • Placing servers containing cardholder data behind proxy servers/firewalls, • Removal or filtering of route advertisements for private networks that employ registered addressing, • Internal use of RFC1918 address space instead of registered addresses.	▪ Examine firewall and router configurations	☐	☐	☐	☒	☐
	(b) Is any disclosure of private IP addresses and routing information to external entities authorized?	▪ Examine firewall and router configurations ▪ Interview personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
1.4	(a) Is personal firewall software installed and active on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network?	▪ Review policies and configuration standards ▪ Examine mobile and/or employee-owned devices	☐	☐	☐	☒	☐
	(b) Is the personal firewall software configured to specific configuration settings, actively running, and not alterable by users of mobile and/or employee-owned devices?	▪ Review policies and configuration standards ▪ Examine mobile and/or employee-owned devices	☐	☐	☐	☒	☐
1.5	Are security policies and operational procedures for managing firewalls: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Review security policies and operational procedures ▪ Interview personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
2.1	(a) Are vendor-supplied defaults always changed before installing a system on the network? *This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).*	▪ Review policies and procedures ▪ Examine vendor documentation ▪ Observe system configurations and account settings ▪ Interview personnel	☐	☐	☐	☐	☐
	(b) Are unnecessary default accounts removed or disabled before installing a system on the network?	▪ Review policies and procedures ▪ Review vendor documentation ▪ Examine system configurations and account settings ▪ Interview personnel	☐	☐	☐	☒	☐
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, are ALL wireless vendor defaults changed at installations, as follows:						
	(a) Are encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions?	▪ Review policies and procedures ▪ Review vendor documentation ▪ Interview personnel	☐	☐	☐	☒	☐
	(b) Are default SNMP community strings on wireless devices changed at installation?	▪ Review policies and procedures ▪ Review vendor documentation ▪ Interview personnel ▪ Examine system configurations	☐	☐	☐	☒	☐
	(c) Are default passwords/passphrases on access points changed at installation?	▪ Review policies and procedures ▪ Interview personnel ▪ Examine system configurations	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
	(d) Is firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks?	▪ Review policies and procedures ▪ Review vendor documentation ▪ Examine system configurations	☐	☐	☐	☒	☐
	(e) Are other security-related wireless vendor defaults changed, if applicable?	▪ Review policies and procedures ▪ Review vendor documentation ▪ Examine system configurations	☐	☐	☐	☒	☐
2.2	(a) Are configuration standards developed for all system components and are they consistent with industry-accepted system hardening standards? *Sources of industry-accepted system hardening standards may include, but are not limited to, SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO), and Center for Internet Security (CIS).*	▪ Review system configuration standards ▪ Review industry-accepted hardening standards ▪ Review policies and procedures ▪ Interview personnel	☐	☐	☐	☐	☐
	(b) Are system configuration standards updated as new vulnerability issues are identified, as defined in Requirement 6.1?	▪ Review policies and procedures ▪ Interview personnel	☐	☐	☐	☐	☐
	(c) Are system configuration standards applied when new systems are configured?	▪ Review policies and procedures ▪ Interview personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
	(d) Do system configuration standards include all of the following: • Changing of all vendor-supplied defaults and elimination of unnecessary default accounts? • Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server? • Enabling only necessary services, protocols, daemons, etc., as required for the function of the system? • Implementing additional security features for any required services, protocols or daemons that are considered to be insecure? • Configuring system security parameters to prevent misuse? • Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers?	▪ Review system configuration standards	☐	☐	☐	☐	☐
2.2.1	(a) Is only one primary function implemented per server, to prevent functions that require different security levels from co-existing on the same server? *For example, web servers, database servers, and DNS should be implemented on separate servers.*	▪ Examine system configurations	☐	☐	☐	☒	☐
	(b) If virtualization technologies are used, is only one primary function implemented per virtual system component or device?	▪ Examine system configurations	☐	☐	☐	☒	☐
2.2.2	(a) Are only necessary services, protocols, daemons, etc. enabled as required for the function of the system (services and protocols not directly needed to perform the device's specified function are disabled)?	▪ Review configuration standards ▪ Examine system configurations	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
	(b) Are all enabled insecure services, daemons, or protocols justified per documented configuration standards?	▪ Review configuration standards ▪ Interview personnel ▪ Examine configuration settings ▪ Compare enabled services, etc. to documented justifications	☐	☐	☐	☒	☐
2.2.3	Are additional security features documented and implemented for any required services, protocols or daemons that are considered to be insecure? *For example, use secured technologies such as SSH, S-FTP, SSL or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.*	▪ Review configuration standards ▪ Examine configuration settings	☐	☐	☐	☒	☐
2.2.4	(a) Are system administrators and/or personnel that configure system components knowledgeable about common security parameter settings for those system components?	▪ Interview personnel	☐	☐	☐	☐	☐
	(b) Are common system security parameters settings included in the system configuration standards?	▪ Review system configuration standards	☐	☐	☐	☐	☐
	(c) Are security parameter settings set appropriately on system components?	▪ Examine system components ▪ Examine security parameter settings ▪ Compare settings to system configuration standards	☐	☐	☐	☐	☐
2.2.5	(a) Has all unnecessary functionality—such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers—been removed?	▪ Examine security parameters on system components	☐	☐	☐	☐	☐
	(b) Are enabled functions documented and do they support secure configuration?	▪ Review documentation ▪ Examine security parameters on system components	☐	☐	☐	☐	☐
	(c) Is only documented functionality present on system components?	▪ Review documentation ▪ Examine security parameters on system components	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
2.3	Is non-console administrative access encrypted as follows: *Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*						
	(a) Is all non-console administrative access encrypted with strong cryptography, and is a strong encryption method invoked before the administrator's password is requested?	▪ Examine system components ▪ Examine system configurations ▪ Observe an administrator log on	☐	☐	☐	☒	☐
	(b) Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands?	▪ Examine system components ▪ Examine services and files	☐	☐	☐	☒	☐
	(c) Is administrator access to web-based management interfaces encrypted with strong cryptography?	▪ Examine system components ▪ Observe an administrator log on	☐	☐	☐	☒	☐
	(d) For the technology in use, is strong cryptography implemented according to industry best practice and/or vendor recommendations?	▪ Examine system components ▪ Review vendor documentation ▪ Interview personnel	☐	☐	☐	☒	☐
2.4	(a) Is an inventory maintained for systems components that are in scope for PCI DSS, including a list of hardware and software components and a description of function/use for each?	▪ Examine system inventory	☐	☐	☐	☐	☐
	(b) Is the documented inventory kept current?	▪ Interview personnel	☐	☐	☐	☐	☐
2.5	Are security policies and operational procedures for managing vendor defaults and other security parameters: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Review security policies and operational procedures ▪ Interview personnel	☐	☐	☐	☐	☐
2.6	*This requirement applies only to service providers.*						

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
3.1	Are data-retention and disposal policies, procedures, and processes implemented as follows:						
	(a) Is data storage amount and retention time limited to that required for legal, regulatory, and business requirements?	▪ Review data retention and disposal policies and procedures ▪ Interview personnel	☐	☐	☐	☒	☐
	(b) Are there defined processes in place for securely deleting cardholder data when no longer needed for legal, regulatory, or business reasons?	▪ Review policies and procedures ▪ Interview personnel ▪ Examine deletion mechanism	☐	☐	☐	☒	☐
	(c) Are there specific retention requirements for cardholder data? *For example, cardholder data needs to be held for X period for Y business reasons.*	▪ Review policies and procedures ▪ Interview personnel ▪ Examine retention requirements	☐	☐	☐	☒	☐
	(d) Is there a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements?	▪ Review policies and procedures ▪ Interview personnel ▪ Observe deletion processes	☐	☐	☐	☒	☐
	(e) Does all stored cardholder data meet the requirements defined in the data-retention policy?	▪ Examine files and system records	☐	☐	☐	☒	☐
3.2	(a) *This testing procedure applies only to Issuers.*						
	(b) *This testing procedure applies only to Issuers.*						
	(c) Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?	▪ Review policies and procedures ▪ Examine system configurations ▪ Examine deletion processes	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
	(d) Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):						
3.2.1	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) are not stored after authorization? *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 cardholder's name,* • *Primary account number (PAN),* • *Expiration date, and* • *Service code* *To minimize risk, store only these data elements as needed for business.*	▪ Examine data sources including: • Incoming transaction data • All logs • History files • Trace files • Database schema • Database contents	☐	☐	☐	☒	☐
3.2.2	The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after authorization?	▪ Examine data sources including: • Incoming transaction data • All logs • History files • Trace files • Database schema • Database contents	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
3.2.3	The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?	▪ Examine data sources including: • Incoming transaction data • All logs • History files • Trace files • Database schema • Database contents	☐	☐	☐	☒	☐
3.3	Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see the full PAN? ***Note:*** *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*	▪ Review policies and procedures ▪ Review roles that need access to displays of full PAN ▪ Examine system configurations ▪ Observe displays of PAN	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
3.4	Is PAN rendered unreadable anywhere it is stored (including data repositories, portable digital media, backup media, and in audit 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. ***Note:*** *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 present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	▪ Examine vendor documentation ▪ Examine data repositories ▪ Examine removable media ▪ Examine audit logs	☐	☐	☐	☒	☐
3.4.1	If disk encryption (rather than file- or column-level database encryption) is used, is access managed as follows:						
	(a) Is logical access to encrypted file systems managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials)?	▪ Examine system configurations ▪ Observe the authentication process	☐	☐	☐	☒	☐
	(b) Are cryptographic keys stored securely (for example, stored on removable media that is adequately protected with strong access controls)?	▪ Observe processes ▪ Interview personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
	(c) Is cardholder data on removable media encrypted wherever stored? ***Note:*** *If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.*	▪ Examine system configurations ▪ Observe processes	☐	☐	☐	☒	☐
3.5	Are keys used to secure stored cardholder data protected against disclosure and misuse as follows: ***Note:*** *This requirement applies to keys used to encrypt stored cardholder data, and 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.*						
3.5.1	Is access to cryptographic keys restricted to the fewest number of custodians necessary?	▪ Examine user access lists	☐	☐	☐	☒	☐
3.5.2	Are secret and private cryptographic keys used to encrypt/decrypt cardholder data stored in in one (or more) of the following forms at all times? ▪ Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key ▪ Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device) ▪ As at least two full-length key components or key shares, in accordance with an industry-accepted method. ***Note:*** *It is not required that public keys be stored in one of these forms.*	▪ Review documented procedures ▪ Examine system configurations and key storage locations, including for key-encrypting keys	☐	☐	☐	☒	☐
3.5.3	Are cryptographic keys stored in the fewest possible locations?	▪ Examine key-storage locations ▪ Observe processes	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
3.6	(a) Are all key-management processes and procedures fully documented and implemented for cryptographic keys used for encryption of cardholder data?	▪ Review key-management procedures	☐	☐	☐	☒	☐
	(b) *This testing procedure applies only to service providers.*						
	(c) Are key-management processes and procedures implemented to require the following:						
3.6.1	Do cryptographic key procedures include the generation of strong cryptographic keys?	▪ Review key-management procedures ▪ Observe key-generation method	☐	☐	☐	☒	☐
3.6.2	Do cryptographic key procedures include secure cryptographic key distribution?	▪ Review key management procedures ▪ Observe the key-distribution method	☐	☐	☐	☒	☐
3.6.3	Do cryptographic key procedures include secure cryptographic key storage?	▪ Review key-management procedures ▪ Observe the method for secure storage of keys	☐	☐	☐	☒	☐
3.6.4	Do cryptographic key procedures include cryptographic key changes for keys that have reached the end of their defined 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)?	▪ Review key-management procedures ▪ Interview personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
3.6.5	(a) Do cryptographic key procedures include retirement or replacement (for example, archiving, destruction, and/or revocation) of cryptographic keys when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key)?	▪ Review key-management procedures ▪ Interview personnel	☐	☐	☐	☒	☐
	(b) Do cryptographic key procedures include replacement of known or suspected compromised keys?	▪ Review key-management procedures ▪ Interview personnel	☐	☐	☐	☒	☐
	(c) If retired or replaced cryptographic keys are retained, are these keys only used for decryption/verification purposes, and not used for encryption operations?	▪ Review key-management procedures ▪ Interview personnel	☐	☐	☐	☒	☐
3.6.6	If manual clear-text key-management operations are used, do cryptographic key procedures include split knowledge and dual control of cryptographic keys as follows: ▪ Do split knowledge procedures require that key components are under the control of at least two people who only have knowledge of their own key components? AND ▪ Do dual control procedures require that at least two people are required to perform any key management operations and no one person has access to the authentication materials (for example, passwords or keys) of another? ***Note:*** *Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	▪ Review key-management procedures ▪ Interview personnel and/or ▪ Observe processes	☐	☐	☐	☒	☐
3.6.7	Do cryptographic key procedures include the prevention of unauthorized substitution of cryptographic keys?	▪ Review procedures ▪ Interview personnel and/or ▪ Observe processes	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
3.6.8	Are cryptographic key custodians required to formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities?	▪ Review procedures ▪ Review documentation or other evidence	☐	☐	☐	☒	☐
3.7	Are security policies and operational procedures for protecting stored cardholder data: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Review security policies and operational procedures ▪ Interview personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
4.1	(a) Are strong cryptography and security protocols, such as SSL/TLS, SSH or IPSEC, used to safeguard sensitive cardholder data during transmission over open, public networks? *Examples of open, public networks include but are not limited to the Internet; wireless technologies, including 802.11 and Bluetooth; cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA); and General Packet Radio Service (GPRS).*	▪ Review documented standards ▪ Review policies and procedures ▪ Review all locations where CHD is transmitted or received ▪ Examine system configurations	☐	☐	☐	☒	☐
	(b) Are only trusted keys and/or certificates accepted?	▪ Observe inbound and outbound transmissions ▪ Examine keys and certificates	☐	☐	☐	☒	☐
	(c) Are security protocols implemented to use only secure configurations, and to not support insecure versions or configurations?	▪ Examine system configurations	☐	☐	☐	☒	☐
	(d) Is the proper encryption strength implemented for the encryption methodology in use (check vendor recommendations/best practices)?	▪ Review vendor documentation ▪ Examine system configurations	☐	☐	☐	☒	☐
	(e) For SSL/TLS implementations, is SSL/TLS enabled whenever cardholder data is transmitted or received? *For example, for browser-based implementations:* • *"HTTPS" appears as the browser Universal Record Locator (URL) protocol, and* • Cardholder data is only requested if "HTTPS" appears as part of the URL.	▪ Examine system configurations	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
4.1.1	Are industry best practices (for example, IEEE 802.11i) used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment? ***Note:*** *The use of WEP as a security control is prohibited.*	▪ Review documented standards ▪ Review wireless networks ▪ Examine system configuration settings	☐	☐	☐	☒	☐
4.2	(a) Are PANs rendered unreadable or secured with strong cryptography whenever they are sent via end-user messaging technologies (for example, e-mail, instant messaging, or chat)?	▪ Observe processes ▪ Review outbound transmissions	☐	☐	☐	☒	☐
	(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?	▪ Review policies and procedures					
4.3	Are security policies and operational procedures for encrypting transmissions of cardholder data: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Review security policies and operational procedures ▪ Interview personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
5.1	Is anti-virus software deployed on all systems commonly affected by malicious software?	▪ Examine system configurations	☐	☐	☐	☐	☐
5.1.1	Are anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits)?	▪ Review vendor documentation ▪ Examine system configurations	☐	☐	☐	☐	☐
5.1.2	Are periodic evaluations performed to identify and evaluate evolving malware threats in order to confirm whether those systems considered to not be commonly affected by malicious software continue as such?	▪ Interview personnel	☐	☐	☐	☐	☐
5.2	Are all anti-virus mechanisms maintained as follows:						
	(a) Are all anti-virus software and definitions kept current?	▪ Examine policies and procedures ▪ Examine anti-virus configurations, including the master installation ▪ Examine system components	☐	☐	☐	☐	☐
	(b) Are automatic updates and periodic scans enabled and being performed?	▪ Examine anti-virus configurations, including the master installation ▪ Examine system components	☐	☐	☐	☐	☐
	(c) Are all anti-virus mechanisms generating audit logs, and are logs retained in accordance with PCI DSS Requirement 10.7?	▪ Examine anti-virus configurations ▪ Review log retention processes	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
5.3	Are all anti-virus mechanisms: ▪ Actively running? ▪ Unable to be disabled or altered by users? ***Note:*** *Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.*	▪ Examine anti-virus configurations ▪ Examine system components ▪ Observe processes ▪ Interview personnel	☐	☐	☐	☐	☐
5.4	Are security policies and operational procedures for protecting systems against malware: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Review security policies and operational procedures ▪ Interview personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Question		Expected Testing	Response (*Check one response for each question*)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.1	Is there a process to identify security vulnerabilities, including the following: ▪ Using reputable outside sources for vulnerability information? ▪ Assigning a risk ranking to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities? ***Note**: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score and/or the classification by the vendor, and/or type of systems affected.* *Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process or transmit cardholder data.*	▪ Review policies and procedures ▪ Interview personnel ▪ Observe processes	☐	☐	☐	☐	☐
6.2	(a) Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?	▪ Review policies and procedures	☐	☐	☐	☐	☐
	(b) Are critical security patches installed within one month of release? ***Note**: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	▪ Review policies and procedures ▪ Examine system components ▪ Compare list of security patches installed to recent vendor patch lists	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.3	(a) Are software- development processes based on industry standards and/or best practices?	▪ Review software development processes ▪ Observe processes ▪ Interview personnel	☐	☐	☐	☒	☐
	(b) Is information security included throughout the software-development life cycle?	▪ Review software development processes ▪ Observe processes ▪ Interview personnel	☐	☐	☐	☒	☐
	(c) Are software applications developed in accordance with PCI DSS (for example, secure authentication and logging)?	▪ Review software development processes ▪ Observe processes ▪ Interview personnel	☐	☐	☐	☒	☐
	(d) Do software development processes ensure the following at 6.3.1 - 6.3.2:						
6.3.1	Are development, test, and/or custom application accounts, user IDs, and passwords removed before applications become active or are released to customers?	▪ Review software development processes ▪ Interview personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.3.2	Is all custom code reviewed prior to release to production or customers to identify any potential coding vulnerability (using either manual or automated processes as follows: ▪ Are code changes reviewed by individuals other than the originating code author, and by individuals who are knowledgeable about code review techniques and secure coding practices? ▪ Do code reviews ensure code is developed according to secure coding guidelines? ▪ Are appropriate corrections are implemented prior to release? ▪ Are code review results are reviewed and approved by management prior to release? ***Note**: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	▪ Review policies and procedures ▪ Interview personnel ▪ Examine recent changes and change records	☐	☐	☐	☒	☐
6.4	Are change control processes and procedures followed for all changes to system components to include the following:						
6.4.1	(a) Are development/test environments separate from the production environment?	▪ Review change control processes and procedures ▪ Examine network documentation and network device configurations	☐	☐	☐	☒	☐
	(b) Is access control in place to enforce the separation between the development/test environments and the production environment?	▪ Review change control processes and procedures ▪ Examine access control settings	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.4.2	Is there separation of duties between personnel assigned to the development/test environments and those assigned to the production environment?	▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel	☐	☐	☐	☒	☐
6.4.3	Are production data (live PANs) ***not*** used for testing or development?	▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel ▪ Examine test data	☐	☐	☐	☒	☐
6.4.4	Are test data and accounts removed before production systems become active?	▪ Review change control processes and procedures ▪ Observe processes ▪ Interview personnel ▪ Examine production systems	☐	☐	☐	☒	☐
6.4.5	(a) Are change-control procedures for implementing security patches and software modifications documented and require the following? • Documentation of impact • Documented change control approval by authorized parties • Functionality testing to verify that the change does not adversely impact the security of the system • Back-out procedures	▪ Review change control processes and procedures	☐	☐	☐	☒	☐
	(b) Are the following performed and documented for all changes:						
6.4.5.1	Documentation of impact?	▪ Trace changes to change control documentation ▪ Examine change control documentation	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.4.5.2	Documented approval by authorized parties?	▪ Trace changes to change control documentation ▪ Examine change control documentation	☐	☐	☐	☒	☐
6.4.5.3	(a) Functionality testing to verify that the change does not adversely impact the security of the system?	▪ Trace changes to change control documentation ▪ Examine change control documentation	☐	☐	☐	☒	☐
	(b) For custom code changes, testing of updates for compliance with PCI DSS Requirement 6.5 before being deployed into production?	▪ Trace changes to change control documentation ▪ Examine change control documentation	☐	☐	☐	☒	☐
6.4.5.4	Back-out procedures?	▪ Trace changes to change control documentation ▪ Examine change control documentation	☐	☐	☐	☒	☐
6.5	(a) Do software-development processes address common coding vulnerabilities?	▪ Review software-development policies and procedures	☐	☐	☐	☒	☐
	(b) Are developers trained in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory?	▪ Interview personnel ▪ Examine training records					
	(c) Are applications developed based on secure coding guidelines to protect applications from, at a minimum, the following vulnerabilities: ***Note:*** *The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are update d (for example, the Open Web Application Security Project (OWASP) Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*						

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.5.1	Do coding techniques address injection flaws, particularly SQL injection? ***Note:*** *Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.*	▪ Examine software-development policies and procedures ▪ Interview responsible personnel	☐	☐	☐	☒	☐
6.5.2	Do coding techniques address buffer overflow vulnerabilities?	▪ Examine software-development policies and procedures ▪ Interview responsible personnel	☐	☐	☐	☒	☐
6.5.3	Do coding techniques address insecure cryptographic storage?	▪ Examine software-development policies and procedures ▪ Interview responsible personnel	☐	☐	☐	☒	☐
6.5.4	Do coding techniques address insecure communications?	▪ Examine software-development policies and procedures ▪ Interview responsible personnel	☐	☐	☐	☒	☐
6.5.5	Do coding techniques address improper error handling?	▪ Examine software-development policies and procedures ▪ Interview responsible personnel	☐	☐	☐	☒	☐
6.5.6	Do coding techniques address all "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1)?	▪ Examine software-development policies and procedures ▪ Interview responsible personnel	☐	☐	☐	☒	☐
For web applications and application interfaces (internal or external), are applications developed based on secure coding guidelines to protect applications from the following additional vulnerabilities:							
6.5.7	Do coding techniques address cross-site scripting (XSS) vulnerabilities?	▪ Examine software-development policies and procedures ▪ Interview responsible personnel	☐	☐	☐	☒	☐
6.5.8	Do coding techniques address improper access control such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions?	▪ Examine software-development policies and procedures ▪ Interview responsible personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.5.9	Do coding techniques address cross-site request forgery (CSRF)?	▪ Examine software-development policies and procedures ▪ Interview responsible personnel	☐	☐	☐	☒	☐
6.5.10	Do coding techniques address broken authentication and session management? ***Note:*** *Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.*	▪ Examine software-development policies and procedures ▪ Interview responsible personnel	☐	☐	☐	☒	☐
6.6	For public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis, and are these applications protected against known attacks by applying *either* of the following methods? ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, as follows: ○ At least annually ○ After any changes ○ By an organization that specializes in application security ○ That all vulnerabilities are corrected ○ That the application is re-evaluated after the corrections ***Note****: This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* – **OR** – ▪ Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications to continually check all traffic.	▪ Review documented processes ▪ Interview personnel ▪ Examine records of application security assessments ▪ Examine system configuration settings	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
6.7	Are security policies and operational procedures for developing and maintaining secure systems and applications: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Review security policies and operational procedures ▪ Interview personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:						
	▪ Is there a written policy for access control that incorporates the following? • Defining access needs and privilege assignments for each role • Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities, • Assignment of access based on individual personnel's job classification and function • Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved	▪ Examine written access control policy	☐	☐	☐	☐	☐
7.1.1	Are access needs for each role defined, including: ▪ System components and data resources that each role needs to access for their job function? ▪ Level of privilege required (for example, user, administrator, etc.) for accessing resources?	▪ Examine roles and access needs	☐	☐	☐	☒	☐
7.1.2	Is access to privileged user IDs restricted as follows: ▪ To least privileges necessary to perform job responsibilities? ▪ Assigned only to roles that specifically require that privileged access?	▪ Interview personnel ▪ Interview management ▪ Review privileged user IDs	☐	☐	☐	☒	☐
7.1.3	Are access assigned based on individual personnel's job classification and function?	▪ Interview management ▪ Review user IDs	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
7.1.4	Is documented approval by authorized parties required, specifying required privileges?	▪ Review user IDs ▪ Compare with documented approvals ▪ Compare assigned privileges with documented approvals	☐	☐	☐	☐	☐
7.2	Is an access control system in place for system components to restrict access based on a user's need to know, and is it set to "deny all" unless specifically allowed, as follows:						
7.2.1	Are access control systems in place on all system components?	▪ Review vendor documentation ▪ Examine configuration settings	☐	☐	☐	☒	☐
7.2.2	Are access control systems configured to enforce privileges assigned to individuals based on job classification and function?	▪ Review vendor documentation ▪ Examine configuration settings	☐	☐	☐	☒	☐
7.2.3	Do access control systems have a default "deny-all" setting?	▪ Review vendor documentation ▪ Examine configuration settings	☐	☐	☐	☒	☐
7.3	Are security policies and operational procedures for restricting access to cardholder data: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Examine security policies and operational procedures ▪ Interview personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 8: Identify and authenticate access to system components

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
8.1	Are policies and procedures for user identification management controls defined and in place for non-consumer users and administrators on all system components, as follows:						
8.1.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?	▪ Review password procedures ▪ Interview personnel	☐	☐	☐	☐	☐
8.1.2	Are additions, deletions, and modifications of user IDs, credentials, and other identifier objects controlled such that user IDs are implemented only as authorized (including with specified privileges)?	▪ Review password procedures ▪ Examine privileged and general user IDs and associated authorizations ▪ Observe system settings	☐	☐	☐	☐	☐
8.1.3	Is access for any terminated users immediately deactivated or removed?	▪ Review password procedures ▪ Examine terminated users accounts ▪ Review current access lists ▪ Observe returned physical authentication devices	☐	☐	☐	☐	☐
8.1.4	Are inactive user accounts over 90 days old either removed or disabled?	▪ Review password procedures ▪ Observe user accounts	☐	☐	☐	☐	☐
8.1.5	(a) Are accounts used by vendors to access, support, or maintain system components via remote access enabled only during the time period needed and disabled when not in use?	▪ Review password procedures ▪ Interview personnel ▪ Observe processes	☐	☐	☐	☒	☐
	(b) Are vendor remote access accounts monitored when in use?	▪ Interview personnel ▪ Observe processes	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
8.1.6	(a) Are repeated access attempts limited by locking out the user ID after no more than six attempts?	▪ Review password procedures ▪ Examine system configuration settings	☐	☐	☐	☐	☐
	(b) *This testing procedure applies only to service providers.*						
8.1.7	Once a user account is locked out, is the lockout duration set to a minimum of 30 minutes or until an administrator enables the user ID?	▪ Review password procedures ▪ Examine system configuration settings	☐	☐	☐	☐	☐
8.1.8	If a session has been idle for more than 15 minutes, are users required to re-authenticate (for example, re-enter the password) to re-activate the terminal or session?	▪ Review password procedures ▪ Examine system configuration settings	☐	☐	☐	☐	☐
8.2	In addition to assigning a unique ID, is one or more of the following methods employed 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	▪ Review password procedures ▪ Observe authentication processes	☐	☐	☐	☐	☐
8.2.1	(a) Is strong cryptography used to render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components?	▪ Review password procedures ▪ Review vendor documentation ▪ Examine system configuration settings ▪ Observe password files ▪ Observe data transmissions	☐	☐	☐	☐	☐
	(b) *This testing procedure applies only to service providers.*						

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
8.2.2	Is user identity verified before modifying any authentication credential (for example, performing password resets, provisioning new tokens, or generating new keys)?	▪ Review authentication procedures ▪ Observe personnel	☐	☐	☐	☐	☐
8.2.3	(a) Are user password parameters configured to require passwords/passphrases meet the following? • A minimum password length of at least seven characters • Contain both numeric and alphabetic characters Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	▪ Examine system configuration settings to verify password parameters	☐	☐	☐	☐	☐
	(b) *This testing procedure applies only to service providers.*						
8.2.4	(a) Are user passwords/passphrases changed at least every 90 days?	▪ Review password procedures ▪ Examine system configuration settings	☐	☐	☐	☐	☐
	(b) *This testing procedure applies only to service providers.*						
8.2.5	(a) Must an individual submit a new password/phrase that is different from any of the last four passwords/phrases he or she has used?	▪ Review password procedures ▪ Sample system components ▪ Examine system configuration settings	☐	☐	☐	☐	☐
	(b) *This testing procedure applies only to service providers.*						
8.2.6	Are passwords/phrases set to a unique value for each user for first-time use and upon reset, and must each user change their password immediately after the first use?	▪ Review password procedures ▪ Examine system configuration settings ▪ Observe security personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
8.3	Is two-factor authentication incorporated for remote network access originating from outside the network by personnel (including users and administrators) and all third parties (including vendor access for support or maintenance)? ***Note:*** *Two-factor authentication requires that two of the three authentication methods (see PCI DSS Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.* *Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate two-factor authentication.*	▪ Review policies and procedures ▪ Examine system configurations ▪ Observe personnel	☐	☐	☐	☐	☐
8.4	(a) Are authentication procedures and policies documented and communicated to all users?	▪ Review policies and procedures ▪ Review distribution method ▪ Interview personnel ▪ Interview users	☐	☐	☐	☐	☐
	(b) Do authentication procedures and policies include the following? • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions that users should change passwords if there is any suspicion the password could be compromised	▪ Review policies and procedures ▪ Review documentation provided to users	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
8.5	Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows: • Generic user IDs and accounts are disabled or removed; • Shared user IDs for system administration activities and other critical functions do not exist; and • Shared and generic user IDs are not used to administer any system components?	▪ Review policies and procedures ▪ Examine user ID lists ▪ Interview personnel	☐	☐	☐	☐	☐
8.5.1	*This requirement applies only to service providers.*						
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, and certificates, etc.), is the use of these mechanisms assigned as follows? • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access	▪ Review policies and procedures ▪ Interview personnel ▪ Examine system configuration settings and/or physical controls	☐	☐	☐	☒	☐
8.7	Is all access to any database containing cardholder data (including access by applications, administrators, and all other users) restricted as follows:						
	(a) Is all user access to, user queries of, and user actions on (for example, move, copy, delete), the database through programmatic methods only (for example, through stored procedures)?	▪ Review database authentication policies and procedures ▪ Examine database and application configuration settings	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
	(b) Is user direct access to or queries to of databases restricted to database administrators?	▪ Review database authentication policies and procedures ▪ Examine database access control settings ▪ Examine database application configuration settings	☐	☐	☐	☒	☐
	(c) Are application IDs only able to be used by the applications (and not by individual users or other processes)?	▪ Review database authentication policies and procedures ▪ Examine database access control settings ▪ Examine database application configuration settings	☐	☐	☐	☒	☐
8.8	Are security policies and operational procedures for identification and authentication: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Examine security policies and operational procedures ▪ Interview personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 9: Restrict physical access to cardholder data

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.1	Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?	▪ Observe physical access controls ▪ Observe personnel	☐	☐	☐	☒	☐
9.1.1	(a) Are video cameras and/or access-control mechanisms in place to monitor individual physical access to sensitive areas? ***Note:*** *"Sensitive areas" refers to any data center, server room, or any area that houses systems that store cardholder data. This excludes pubic-facing areas where only point-of-sale terminals are present such as the cashier areas in a retail store.*	▪ Review policies and procedures ▪ Observe physical monitoring mechanisms ▪ Observe security features	☐	☐	☐	☒	☐
	(b) Are video cameras and/or access-control mechanisms protected from tampering or disabling?	▪ Observe processes ▪ Interview personnel	☐	☐	☐	☒	☐
	(c) Is data collected from video cameras and/or access control mechanisms reviewed and correlated with other entries?	▪ Review policies and procedures ▪ Interview security personnel					
	(d) Is data collected from video cameras and/or access control mechanisms stored for at least three months unless otherwise restricted by law?	▪ Review data retention processes ▪ Observe data storage ▪ Interview security personnel	☐	☐	☐	☒	☐
9.1.2	Are physical and/or logical controls in place to restrict access to publicly accessible network jacks? *For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.*	▪ Review policies and procedures ▪ Interview personnel ▪ Observe locations	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.1.3	Is physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines restricted?	▪ Review policies and procedures ▪ Interview personnel ▪ Observe devices	☐	☐	☐	☐	☐
9.2	(a) Are procedures developed to easily distinguish between onsite personnel and visitors, which include: • Identifying new onsite personnel or visitors (for example, assigning badges), • Changing access requirements, and • Revoking terminated onsite personnel and expired visitor identification (such as ID badges) *For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day.*	▪ Review policies and procedures ▪ Interview personnel ▪ Observe identification methods (e.g. badges) ▪ Observe visitor processes	☐	☐	☐	☐	☐
	(b) Do identification methods (such as ID badges) clearly identify visitors and easily distinguish between onsite personnel and visitors?	▪ Observe identification methods	☐	☐	☐	☐	☐
	(c) Is access to the badge system limited to authorized personnel?	▪ Observe physical controls and access controls for the badge system	☐	☐	☐	☐	☐
9.3	Is physical access to sensitive areas controlled for onsite personnel, as follows: ▪ Is access authorized and based on individual job function? ▪ Is access revoked immediately upon termination ▪ Upon termination, are all physical access mechanisms, such as keys, access cards, etc., returned or disabled?	▪ Interview personnel ▪ Examine access control lists ▪ Observe onsite personnel ▪ Compare lists of terminated employees to access control lists	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.4	Is visitor identification and access handled as follows:						
9.4.1	Are visitors authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained?	▪ Review policies and procedures ▪ Observe visitor processes including how access is controlled ▪ Interview personnel ▪ Observe visitors and badge use	☐	☐	☐	☒	☐
9.4.2	(a) Are visitors identified and given a badge or other identification that visibly distinguishes the visitors from onsite personnel?	▪ Observe badge use of personnel and visitors ▪ Examine identification	☐	☐	☐	☒	☐
	(b) Do visitor badges or other identification expire?	▪ Observe process ▪ Examine identification	☐	☐	☐	☒	☐
9.4.3	Are visitors asked to surrender the badge or other identification before leaving the facility or at the date of expiration?	▪ Observe processes ▪ Observe visitors leaving facility	☐	☐	☐	☒	☐
9.4.4	(a) Is a visitor log in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted?	▪ Review policies and procedures ▪ Examine the visitor log ▪ Observe visitor processes ▪ Examine log retention	☐	☐	☐	☒	☐
	(b) Does the visitor log contain the visitor's name, the firm represented, and the onsite personnel authorizing physical access?	▪ Review policies and procedures ▪ Examine the visitor log	☐	☐	☐	☒	☐
	(c) Is the visitor log retained for at least three months?	▪ Review policies and procedures ▪ Examine visitor log retention	☐	☐	☐	☒	☐
9.5	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? *For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.*	▪ Review policies and procedures for physically securing media ▪ Interview personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.5.1	(a) Are media back-ups stored in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility?	▪ Observe physical security at media location	☐	☐	☐	☒	☐
	(b) Is this location's security reviewed at least annually?	▪ Review policies and procedures for reviewing offsite media locations ▪ Interview security personnel	☐	☐	☐	☒	☐
9.6	(a) Is strict control maintained over the internal or external distribution of any kind of media?	▪ Review policies and procedures for distribution of media	☐	☐	☐	☒	☐
	(b) Do controls include the following:						
9.6.1	Is media classified so the sensitivity of the data can be determined?	▪ Review policies and procedures for media classification ▪ Interview security personnel	☐	☐	☐	☒	☐
9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	▪ Interview personnel ▪ Examine media distribution tracking logs and documentation	☐	☐	☐	☒	☐
9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	▪ Interview personnel ▪ Examine media distribution tracking logs and documentation	☐	☐	☐	☒	☐
9.7	Is strict control maintained over the storage and accessibility of media?	▪ Review policies and procedures	☐	☐	☐	☒	☐
9.7.1	(a) Are inventory logs of all media properly maintained?	▪ Examine inventory logs	☐	☐	☐	☒	☐
	(b) Are periodic media inventories conducted at least annually?	▪ Examine inventory logs ▪ Interview personnel	☐	☐	☐	☒	☐
9.8	(a) Is all media destroyed when it is no longer needed for business or legal reasons?	▪ Review periodic media destruction policies and procedures	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
	(b) Is there a periodic media destruction policy that defines requirements for the following? • Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. • Storage containers used for materials that are to be destroyed must be secured. • Cardholder data on electronic media must be rendered unrecoverable via a secure wipe program (in accordance with industry-accepted standards for secure deletion), or by physically destroying the media.	▪ Review periodic media destruction policies and procedures	☐	☐	☐	☐	☐
	(c) Is media destruction performed as follows:						
9.8.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	▪ Interview personnel ▪ Examine procedures ▪ Observe processes	☐	☐	☐	☐	☐
	(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	▪ Examine security of storage containers	☐	☐	☐	☐	☐
9.8.2	Is cardholder data on electronic media rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise by physically destroying the media, so that cardholder data cannot be reconstructed?	▪ Observe processes ▪ Interview personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.9	Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows? ***Note:*** *This requirement applies to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.* ***Note:*** *Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement.*						
	(a) Do policies and procedures require that a list of such devices maintained?	▪ Review policies and procedures	☐	☐	☐	☐	☐
	(b) Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?	▪ Review policies and procedures	☐	☐	☐	☐	☐
	(c) Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?	▪ Review policies and procedures	☐	☐	☐	☐	☐
9.9.1	(a) Does the list of devices include the following? • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification	▪ Examine the list of devices	☐	☐	☐	☐	☐
	(b) Is the list accurate and up to date?	▪ Observe device locations and compare to list	☐	☐	☐	☐	☐
	(c) Is the list of devices updated when devices are added, relocated, decommissioned, etc.?	▪ Interview personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
9.9.2	(a) Are device surfaces periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) as follows? ***Note:*** *Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.*	▪ Interview personnel ▪ Observe inspection processes and compare to defined processes	☐	☐	☐	☐	☐
	(b) Are personnel are aware of procedures for inspecting devices?	▪ Interview personnel	☐	☐	☐	☐	☐
9.9.3	Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?						•
	(a) Do training materials for personnel at point-of-sale locations include the following? • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	▪ Review training materials	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
	(b) Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices?	▪ Interview personnel at POS locations	☐	☐	☐	☐	☐
9.10	Are security policies and operational procedures for restricting physical access to cardholder data: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Examine security policies and operational procedures ▪ Interview personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
10.1	(a) Are audit trails enabled and active for system components?	▪ Observe processes ▪ Interview system administrator	☐	☐	☐	☒	☐
	(b) Is access to system components linked to individual users?	▪ Observe processes ▪ Interview system administrator	☐	☐	☐	☒	☐
10.2	Are automated audit trails implemented for all system components to reconstruct the following events:						
10.2.1	All individual user accesses to cardholder data?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	☐	☐	☐	☒	☐
10.2.2	All actions taken by any individual with root or administrative privileges?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	☐	☐	☐	☒	☐
10.2.3	Access to all audit trails?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	☐	☐	☐	☒	☐
10.2.4	Invalid logical access attempts?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	☐	☐	☐	☒	☐
10.2 5	Use of and changes to identification and authentication mechanisms–including but not limited to creation of new accounts and elevation of privileges – and all changes, additions, or deletions to accounts with root or administrative privileges?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
10.2.6	Initialization, stopping, or pausing of the audit logs?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	☐	☐	☐	☒	☐
10.2.7	Creation and deletion of system-level object?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	☐	☐	☐	☒	☐
10.3	Are the following audit trail entries recorded for all system components for each event:						
10.3.1	User identification?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	☐	☐	☐	☒	☐
10.3.2	Type of event?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	☐	☐	☐	☒	☐
10.3.3	Date and time?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	☐	☐	☐	☒	☐
10.3.4	Success or failure indication?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	☐	☐	☐	☒	☐
10.3.5	Origination of event?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	☐	☐	☐	☒	☐
10.3.6	Identity or name of affected data, system component, or resource?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
10.4	Are all critical system clocks and times synchronized through use of time synchronization technology, and is the technology kept current? ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*	▪ Review time configuration standards and processes	☐	☐	☐	☒	☐
10.4.1	Are the following processes implemented for critical systems to have the correct and consistent time:						•
	(a) Do only designated central time server(s) receive time signals from external sources, and are time signals from external sources based on International Atomic Time or UTC?	▪ Review time configuration standards and processes ▪ Examine time-related system parameters	☐	☐	☐	☒	☐
	(b) Where there is more than one designated time server, do the time servers peer with each other to keep accurate time?	▪ Review time configuration standards and processes ▪ Examine time-related system parameters	☐	☐	☐	☒	☐
	(c) Do systems receive time only from designated central time server(s)?	▪ Review time configuration standards and processes ▪ Examine time-related system parameters	☐	☐	☐	☒	☐
10.4.2	Is time data is protected as follows: (a) Is access to time data restricted to only personnel with a business need to access time data?	▪ Examine system configurations and time-synchronization settings	☐	☐	☐	☒	☐
	(b) Are changes to time settings on critical systems logged, monitored, and reviewed?	▪ Examine system configurations and time-synchronization settings and logs	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
10.4.3	Are time settings received from specific, industry-accepted time sources? (This is to prevent a malicious individual from changing the clock). *Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).*	▪ Examine system configurations	☐	☐	☐	☒	☐
10.5	Are audit trails secured so they cannot be altered, as follows:						
10.5.1	Is viewing of audit trails limited to those with a job-related need?	▪ Interview system administrators ▪ Examine system configurations and permissions	☐	☐	☐	☒	☐
10.5.2	Are audit trail files protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation?	▪ Interview system administrators ▪ Examine system configurations and permissions	☐	☐	☐	☒	☐
10.5.3	Are audit trail files promptly backed up to a centralized log server or media that is difficult to alter?	▪ Interview system administrators ▪ Examine system configurations and permissions	☐	☐	☐	☒	☐
10.5.4	Are logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) written onto a secure, centralized, internal log server or media?	▪ Interview system administrators ▪ Examine system configurations and permissions	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
10.5.5	Is file-integrity monitoring or change-detection software used on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)?	▪ Examine settings, monitored files, and results from monitoring activities	☐	☐	☐	☒	☐
10.6	Are logs and security events for all system components reviewed to identify anomalies or suspicious activity as follows? ***Note:*** *Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.*						
10.6.1	(a) Are written policies and procedures defined for reviewing the following at least daily, either manually or via log tools? • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	▪ Review security policies and procedures	☐	☐	☐	☒	☐
	(b) Are the above logs and security events reviewed at least daily?	▪ Observe processes ▪ Interview personnel	☐	☐	☐	☒	☐
10.6.2	(a) Are written policies and procedures defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization's policies and risk management strategy?	▪ Review security policies and procedures	☐	☐	☐	☒	☐
	(b) Are reviews of all other system components performed in accordance with organization's policies and risk management strategy?	▪ Review risk assessment documentation ▪ Interview personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
10.6.3	(a) Are written policies and procedures defined for following up on exceptions and anomalies identified during the review process?	▪ Review security policies and procedures	☐	☐	☐	☒	☐
	(b) Is follow up to exceptions and anomalies performed?	▪ Observe processes ▪ Interview personnel	☐	☐	☐	☒	☐
10.7	(a) Are audit log retention policies and procedures in place and do they require that logs are retained for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup)?	▪ Review security policies and procedures	☐	☐	☐	☒	☐
	(b) Are audit logs retained for at least one year?	▪ Interview personnel ▪ Examine audit logs	☐	☐	☐	☒	☐
	(c) Are at least the last three months' logs immediately available for analysis?	▪ Interview personnel ▪ Observe processes	☐	☐	☐	☒	☐
10.8	Are security policies and operational procedures for monitoring all access to network resources and cardholder data: ▪ Documented ▪ In use ▪ Known to all affected parties?	▪ Review security policies and operational procedures ▪ Interview personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Requirement 11: Regularly test security systems and processes

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
11.1	(a) Are processes implemented for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis? ***Note:*** *Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.*	▪ Review policies and procedures	☐	☐	☐	☒	☐
	(b) Does the methodology detect and identify any unauthorized wireless access points, including at least the following? • WLAN cards inserted into system components; • Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.); and • Wireless devices attached to a network port or network device.	▪ Evaluate the methodology	☐	☐	☐	☒	☐
	(c) Is the scan to identify authorized and unauthorized wireless access points performed at least quarterly for all system components and facilities?	▪ Examine output from recent wireless scans	☐	☐	☐	☒	☐
	(d) If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), is monitoring configured to generate alerts to notify personnel?	▪ Examine configuration settings	☐	☐	☐	☒	☐
11.1.1	Is an inventory of authorized wireless access points maintained and a business justification documented for all authorized wireless access points?	▪ Examine inventory records	☐	☐	☐	☒	☐
11.1.2	(a) Does the incident response plan define and require a response in the event that an unauthorized wireless access point is detected?	▪ Examine incident response plan (see Requirement 12.10)	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
	(b) Is action taken when unauthorized wireless access points are found?	▪ Interview responsible personnel ▪ Inspect recent wireless scans and related responses	☐	☐	☐	☒	☐
11.2	Are internal and external network vulnerability scans run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), as follows? ***Note:*** *Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.* *For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*						
11.2.1	(a) Are quarterly internal vulnerability scans performed?	▪ Review scan reports	☐	☐	☐	☒	☐
	(b) Does the quarterly internal scan process include rescans as needed until all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved?	▪ Review scan reports	☐	☐	☐	☒	☐
	(c) Are quarterly internal scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	▪ Interview personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
11.2.2	(a) Are quarterly external vulnerability scans performed? ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).* *Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	▪ Review results from the four most recent quarters of external vulnerability scans	☐	☐	☐	☒	☐
	(b) Do external quarterly scan and rescan results satisfy the *ASV Program Guide* requirements for a passing scan (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures)?	▪ Review results of each external quarterly scan and rescan	☐	☐	☐	☒	☐
	(c) Are quarterly external vulnerability scans performed by a PCI SSC Approved Scanning Vendor (ASV?	▪ Review results of each external quarterly scan and rescan	☐	☐	☐	☒	☐
11.2.3	(a) Are internal and external scans, and rescans as needed, performed after any significant change? ***Note:*** *Scans must be performed by qualified personnel.*	▪ Examine and correlate change control documentation and scan reports	☐	☐	☐	☒	☐
	(b) Does the scan process include rescans until: • For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS, • For internal scans, a passing result is obtained or all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved?	▪ Review scan reports	☐	☐	☐	☒	☐
	(c) Are scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	▪ Interview personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
11.3	Does the penetration-testing methodology include the following? ▪ Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) ▪ Includes coverage for the entire CDE perimeter and critical systems ▪ Includes testing from both inside and outside the network ▪ Includes testing to validate any segmentation and scope-reduction controls ▪ Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 ▪ Defines network-layer penetration tests to include components that support network functions as well as operating systems ▪ Includes review and consideration of threats and vulnerabilities experienced in the last 12 months ▪ Specifies retention of penetration testing results and remediation activities results	▪ Examine penetration-testing methodology ▪ Interview responsible personnel	☐	☐	☐	☒	☐
11.3.1	(a) Is *external* penetration testing performed per the defined methodology, at least annually, and after any significant infrastructure or application changes to the environment (such as an operating system upgrade, a sub-network added to the environment, or an added web server)?	▪ Examine scope of work ▪ Examine results from the most recent external penetration test	☐	☐	☐	☒	☐
	(b) Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	▪ Examine scope of work ▪ Interview responsible personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
11.3.2	(a) Is *internal* penetration testing performed per the defined methodology, at least annually, and after any significant infrastructure or application changes to the environment (such as an operating system upgrade, a sub-network added to the environment, or an added web server)?	▪ Examine scope of work ▪ Examine results from the most recent internal penetration test	☐	☐	☐	☒	☐
	(b) Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	▪ Examine scope of work ▪ Interview responsible personnel	☐	☐	☐	☒	☐
11.3.3	Are exploitable vulnerabilities found during penetration testing corrected, followed by repeated testing to verify the corrections?	▪ Examine penetration testing results	☐	☐	☐	☒	☐
11.3.4	If segmentation is used to isolate the CDE from other networks: (a) Are penetration-testing procedures defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from in-scope systems?	▪ Examine segmentation controls ▪ Review penetration-testing methodology	☐	☐	☐	☒	☐
	(b) Does penetration testing to verify segmentation controls meet the following? • Performed at least annually and after any changes to segmentation controls/methods • Covers all segmentation controls/methods in use • Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.	▪ Examine results from the most recent penetration test	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
11.4	(a) Are intrusion-detection and/or intrusion-prevention techniques that detect and/or prevent intrusions into the network in place to monitor all traffic: • At the perimeter of the cardholder data environment, and • At critical points in the cardholder data environment.	▪ Examine system configurations ▪ Examine network diagrams	☐	☐	☐	☒	☐
	(b) Are intrusion-detection and/or intrusion-prevention techniques configured to alert personnel of suspected compromises?	▪ Examine system configurations ▪ Interview responsible personnel	☐	☐	☐	☒	☐
	(c) Are all intrusion-detection and prevention engines, baselines, and signatures kept up-to-date?	▪ Examine IDS/IPS configurations ▪ Examine vendor documentation	☐	☐	☐	☒	☐
11.5	(a) Is a change-detection mechanism (for example, file-integrity monitoring tools) deployed within the cardholder data environment to detect unauthorized modification of critical system files, configuration files, or content files? *Examples of files that should be monitored include:* • *System executables* • *Application executables* • *Configuration and parameter files* • *Centrally stored, historical or archived, log, and audit files* • *Additional critical files determined by entity (for example, through risk assessment or other means)*	▪ Observe system settings and monitored files ▪ Examine system configuration settings	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
	(b) Is the change-detection mechanism configured to alert personnel to unauthorized modification of critical system files, configuration files or content files, and do the tools perform critical file comparisons at least weekly? ***Note:*** *For change detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).*	▪ Observe system settings and monitored files ▪ Review results from monitoring activities	☐	☐	☐	☒	☐
11.5.1	Is a process in place to respond to any alerts generated by the change-detection solution?	▪ Examine system configuration settings	☐	☐	☐	☒	☐
11.6	Are security policies and operational procedures for security monitoring and testing: • Documented • In use • Known to all affected parties?	▪ Examine security policies and operational procedures ▪ Interview personnel	☐	☐	☐	☒	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

Note: *For the purposes of Requirement 12, "personnel" refers to full-time part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site or otherwise have access to the company's site cardholder data environment.*

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel?	▪ Review the information security policy	☐	☐	☐	☐	☐
12.1.1	Is the security policy reviewed at least annually and updated when the environment changes?	▪ Review the information security policy ▪ Interview responsible personnel	☐	☐	☐	☐	☐
12.2	(a) Is an annual risk assessment process implemented that identifies assets, threats, and vulnerabilities? *Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.*	▪ Review annual risk assessment process ▪ Interview personnel	☐	☐	☐	☐	☐
	(b) Does the risk assessment process result in a formal risk assessment?	▪ Review the formal risk assessment	☐	☐	☐	☐	☐
	(c) Is the risk assessment process performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.)?	▪ Review risk assessment documentation ▪ Interview responsible personnel	☐	☐	☐	☐	☐
12.3	Are usage policies for critical technologies developed to define proper use of these technologies and require the following: ***Note:*** *Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.*						
12.3.1	Explicit approval by authorized parties to use the technologies?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.3.2	Authentication for use of the technology?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐	☐
12.3.3	A list of all such devices and personnel with access?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐	☐
12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐	☐
12.3.5	Acceptable uses of the technologies?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐	☐
12.3.6	Acceptable network locations for the technologies?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐	☐
12.3.7	List of company-approved products?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐	☐
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐	☐
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐	☐
12.3.10	(a) For personnel accessing cardholder data via remote-access technologies, does the policy specify the prohibition of copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need? *Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.*	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
	(b) For personnel with proper authorization, does the policy require the protection of cardholder data in accordance with PCI DSS Requirements?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐	☐
12.4	Do security policy and procedures clearly define information security responsibilities for all personnel?	▪ Review information security policy and procedures ▪ Interview a sample of responsible personnel	☐	☐	☐	☐	☐
12.5	(a) Is responsibility for information security formally assigned to a Chief Security Officer or other security-knowledgeable member of management?	▪ Review information security policy and procedures	☐	☐	☐	☐	☐
	(b) Are the following information security management responsibilities formally assigned to an individual or team:						
12.5.1	Establishing, documenting, and distributing security policies and procedures?	▪ Review information security policy and procedures	☐	☐	☐	☐	☐
12.5.2	Monitoring and analyzing security alerts and information, and distributing to appropriate personnel?	▪ Review information security policy and procedures	☐	☐	☐	☐	☐
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	▪ Review information security policy and procedures	☐	☐	☐	☐	☐
12.5.4	Administering user accounts, including additions, deletions, and modifications?	▪ Review information security policy and procedures	☐	☐	☐	☐	☐
12.5.5	Monitoring and controlling all access to data?	▪ Review information security policy and procedures	☐	☐	☐	☐	☐
12.6	(a) Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?	▪ Review security awareness program	☐	☐	☐	☐	☐
	(b) Do security awareness program procedures include the following:						

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.6.1	(a) Does the security awareness program provide multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions)? ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*	▪ Review security awareness program ▪ Review security awareness program procedures ▪ Review security awareness program attendance records	☐	☐	☐	☐	☐
	(b) Are personnel educated upon hire and at least annually?	▪ Examine security awareness program procedures and documentation	☐	☐	☐	☐	☐
	(c) Have employees completed awareness training and are they aware of the importance of cardholder data security?	▪ Interview personnel	☐	☐	☐	☐	☐
12.6.2	Are personnel required to acknowledge at least annually that they have read and understood the security policy and procedures?	▪ Examine security awareness program procedures and documentation	☐	☐	☐	☐	☐
12.7	Are potential personnel (see definition of "personnel" above) screened prior to hire to minimize the risk of attacks from internal sources? *Examples of background checks include previous employment history, criminal record, credit history and reference checks.* ***Note:*** *For those potential personnel to be hired for certain positions, such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	▪ Interview Human Resource department management	☐	☐	☐	☐	☐
12.8	Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:						

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.8.1	Is a list of service providers maintained?	▪ Review policies and procedures ▪ Observe processes ▪ Review list of service providers	☐	☐	☐	☒	☐
12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment? ***Note:*** *The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	▪ Observe written agreements ▪ Review policies and procedures	☐	☐	☐	☒	☐
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	▪ Observe processes ▪ Review policies and procedures and supporting documentation	☐	☐	☐	☒	☐
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	▪ Observe processes ▪ Review policies and procedures and supporting documentation	☐	☐	☐	☒	☐
12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	▪ Observe processes ▪ Review policies and procedures and supporting documentation	☐	☐	☐	☒	☐
12.9	*This requirement applies only to service providers.*						
12.10	Has an incident response plan been implemented in preparation to respond immediately to a system breach, as follows:						

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.10.1	(a) Has an incident response plan been created to be implemented in the event of system breach?	▪ Review the incident response plan ▪ Review incident response plan procedures	☐	☐	☐	☐	☐
	(b) Does the plan address the following, at a minimum:						
	• Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum?	▪ Review incident response plan procedures	☐	☐	☐	☐	☐
	• Specific incident response procedures?	▪ Review incident response plan procedures	☐	☐	☐	☐	☐
	• Business recovery and continuity procedures?	▪ Review incident response plan procedures	☐	☐	☐	☐	☐
	• Data backup processes?	▪ Review incident response plan procedures	☐	☐	☐	☐	☐
	• Analysis of legal requirements for reporting compromises?	▪ Review incident response plan procedures	☐	☐	☐	☐	☐
	• Coverage and responses of all critical system components?	▪ Review incident response plan procedures	☐	☐	☐	☐	☐
	• Reference or inclusion of incident response procedures from the payment brands?	▪ Review incident response plan procedures	☐	☐	☐	☐	☐
12.10.2	Is the plan tested at least annually?	▪ Review incident response plan procedures ▪ Interview responsible personnel	☐	☐	☐	☐	☐
12.10.3	Are specific personnel designated to be available on a 24/7 basis to respond to alerts?	▪ Observe processes ▪ Review policies ▪ Interview responsible personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question		Expected Testing	Response (Check one response for each question)				
			Yes	Yes with CCW	No	N/A	Not Tested
12.10.4	Is appropriate training provided to staff with security breach response responsibilities?	▪ Observe processes ▪ Review incident response plan procedures ▪ Interview responsible personnel	☐	☐	☐	☐	☐
12.10.5	Are alerts from security monitoring systems, including intrusion-detection, intrusion-prevention, and file-integrity monitoring systems, included in the incident response plan?	▪ Observe processes ▪ Review incident response plan procedures	☐	☐	☐	☐	☐
12.10.6	Is a process developed and in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments?	▪ Observe processes ▪ Review incident response plan procedures ▪ Interview responsible personnel	☐	☐	☐	☐	☐

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

This appendix is not used for merchant assessments.

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix B: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where "YES with CCW" was checked.

Note: *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Refer to Appendices B, C, and D of PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix C: Explanation of Non-Applicability

If the "N/A" (Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
3.4	Cardholder data is never stored electronically
1.X, 2.1(a), 2.1.1, 2.2.1, 2.3, 3.1 - 3.2.1, 3.2.3, 3.4, - 3.6.8, 4.X, 7.1 - 7.1.3, 7.2.X, 8.6 - 8.7, 9.1 - 9.1.2, 9.3 - 9.4.4, 9.5.1 - 9.7.X, 10.X, 11.X	Using Chase Paymentech guaranteed E2EE solution on secured mobile device.
2.2.2(b), 2.2.3	No unsecured applications enabled.
6.3 - 6.6	No development of applications.
12.8.X	No Service Providers utilized. Paymentech is our acquiring bank.
8.1.5	No vendors have access.

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix D: Explanation of Requirements Not Tested

If the "Not Tested" column was checked in the questionnaire, use this worksheet to explain why the related requirement was not reviewed as part of the assessment.

Requirement	Describe which part(s) of the requirement was not tested	Describe why requirements were not tested
Examples:		
Requirement 12	*Requirement 12.2 was the only requirement tested. All other requirements from Requirement 12 were excluded.*	*This assessment only covers requirements in Milestone 1 of the Prioritized Approach.*
Requirements 1-8, 10-12	*Only Requirement 9 was reviewed for this assessment. All other requirements were excluded.*	*Company is a physical hosting provider (CO-LO), and only physical security controls were considered for this assessment.*

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the SAQ D dated *(completion date)*, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document as of *(date)*: (***check one):***

☐	**Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *(Merchant Company Name)* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Merchant Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "No" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☐	PCI DSS Self-Assessment Questionnaire D, Version *(version of SAQ)*, was completed according to the instructions therein.
☐	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☐	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☐	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Part 3a. Acknowledgement of Status (continued)	
☐	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☐	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *(ASV Name)*

Part 3b. Merchant Attestation	
Signature of Merchant Executive Officer ↑	*Date:*
Merchant Executive Officer Name:	*Title:*

Part 3c. QSA Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	

Signature of QSA ↑	*Date:*
QSA Name:	*QSA Company:*

Part 3d. ISA Acknowledgement (if applicable)	
If a ISA was involved or assisted with this assessment, describe the role performed:	

Signature of ISA ↑	*Date:*
ISA Name:	*Title:*

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with your acquirer or the payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☐	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☐	☐	
3	Protect stored cardholder data	☐	☐	
4	Encrypt transmission of cardholder data across open, public networks	☐	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☐	☐	
6	Develop and maintain secure systems and applications	☐	☐	
7	Restrict access to cardholder data by business need to know	☐	☐	
8	Identify and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Track and monitor all access to network resources and cardholder data	☐	☐	
11	Regularly test security systems and processes	☐	☐	
12	Maintain a policy that addresses information security for all personnel	☐	☐	

© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved.