Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire A-EP and Attestation of Compliance

Partially Outsourced E-commerce Merchants Using a Third-Party Website for Payment Processing

Version 3.1

June 2015

Document Changes

Date	Version	Description
N/A	1.0	Not used.
N/A	2.0	Not used.
February 2014	3.0	New SAQ to address requirements applicable to e-commerce merchants with a website(s) that does not itself receive cardholder data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data. Content aligns with PCI DSS v3.0 requirements and testing procedures.
April 2015	3.1	Updated to align with PCI DSS v3.1. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1*.
June 2015	3.1	Update Requirement 11.3 to fix error.

Table of Contents

Before You Begin

SAQ A-EP has been developed to address requirements applicable to e-commerce merchants with a website(s) that does not itself receive cardholder data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data.

SAQ A-EP merchants are e-commerce merchants who partially outsource their e-commerce payment channel to PCI DSS validated third parties and do not electronically store, process, or transmit any cardholder data on their systems or premises.

SAQ A-EP merchants confirm that, for this payment channel:

- Your company accepts only e-commerce transactions;
- All processing of cardholder data, with the exception of the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor;
- Your e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor;
- If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider);
- Each element of the payment page(s) delivered to the consumer's browser originates from either the merchant's website or a PCI DSS compliant service provider(s);
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions;
- Your company has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

This SAQ is applicable only to e-commerce channels.

This shortened version of the SAQ includes questions that apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

Note: *For the purposes of this SAQ, PCI DSS requirements that refer to the "cardholder data environment" are applicable to the merchant website(s). This is because the merchant website directly impacts how the payment card data is transmitted, even though the website itself does not receive cardholder data.*

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 (as defined in Part 2g of the Attestation of Compliance).
3. Assess your environment for compliance with applicable 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 A-EP)
   - 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
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.

Guidance for Non-Applicability of Certain, Specific Requirements

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.

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.

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) □ E-Commerce □ Card-present (face-to-face)	□ Mail order/telephone order (MOTO) □ E-Commerce □ 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.*

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

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
Example: Retail outlets	*3*	*Boston, MA, USA*

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)
			□ 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.*	
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

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.*

Part 2g. Eligibility to Complete SAQ A-EP	
Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:	
□	Merchant accepts only e-commerce transactions;
□	All processing of cardholder data, with the exception of the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor;
□	Merchant's e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor;
□	If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider);
□	Each element of the payment page(s) delivered to the consumer's browser originates from either the merchant's website or a PCI DSS compliant service provider(s);
□	Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;
□	Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
□	Merchant retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

Section 2: Self-Assessment Questionnaire A-EP

***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

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
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	□	□	□	□
	(b) Is the current network diagram consistent with the firewall configuration standards?	▪ Compare firewall configuration standards to current network diagram	□	□	□	□
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	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	**Yes with CCW**	**No**	**N/A**
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.*					
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	□	□	□	□
1.3.4	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	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
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	□	□	□	□

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
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	□	□	□	□
2.2	(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	□	□	□	□

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
	(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	□	□	□	□

	PCI DSS Question	Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
	(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, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.* ***Note:** SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.* *Effective immediately, new implementations must not use SSL or early TLS.* *POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.*	▪ Review configuration standards ▪ Examine configuration settings *If SSL/early TLS is used:* ▪ Review documentation that verifies POS POI devices are not susceptible to any known exploits for SSL/early TLS *and/or* ▪ Review Risk Mitigation and Migration Plan	□	□	□	□
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	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	**Yes with CCW**	**No**	**N/A**
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	□	□	□	□
2.3	Is non-console administrative access encrypted as follows: *Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.* ***Note:*** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.* *Effective immediately, new implementations must not use SSL or early TLS.* POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.					
	(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	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
	(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	□	□	□	□
	(b) *For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:* Is there documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS?	▪ Review documentation that verifies POS POI devices are not susceptible to any known exploits for SSL/early TLS	□	□	□	□
	(f) *For all other environments using SSL and/or early TLS:* Does the documented Risk Mitigation and Migration Plan include the following? ▪ Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; ▪ Risk assessment results and risk reduction controls in place; ▪ Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; ▪ Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; Overview of migration project plan including target migration completion date no later than 30th June 2016.	▪ Review Risk Mitigation and Migration Plan	□	□	□	□

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**
3.2	(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	□	□	□	□
	(d) Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):					
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	□	□	□	□
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	□	□	□	□

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
4.1	(a) Are strong cryptography and security protocols, such as 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).* **Note:** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.* *Effective immediately, new implementations must not use SSL or early TLS.* POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.	▪ 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	□	□	□	□

	PCI DSS Question	Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
	(e) For TLS implementations, is 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	□	□	□	□
	(f) *For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:* Is there documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS?	▪ Review documentation that verifies POS POI devices are not susceptible to any known exploits for SSL/early TLS	□	□	□	□
	(g) *For all other environments using SSL and/or early TLS:* Does the documented Risk Mitigation and Migration Plan include the following? ▪ Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; ▪ Risk assessment results and risk reduction controls in place; ▪ Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; ▪ Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; ▪ Overview of migration project plan including target migration completion date no later than 30th June 2016.	▪ Review Risk Mitigation and Migration Plan	□	□	□	□

<table>
<tr><th colspan="2" rowspan="2">PCI DSS Question</th><th rowspan="2">Expected Testing</th><th colspan="4">Response
<em>(Check one response for each question)</em></th></tr>
<tr><th>Yes</th><th>Yes with CCW</th><th>No</th><th>N/A</th></tr>
<tr><td>4.2</td><td>(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?</td><td>▪ Review policies and procedures</td><td>□</td><td>□</td><td>□</td><td>□</td></tr>
</table>

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
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	□	□	□	□

PCI DSS Question		Expected Testing	Response (*Check one response for each question*)			
			Yes	**Yes with CCW**	**No**	**N/A**
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	□	□	□	□

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
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	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
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	□	□	□	□
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	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
6.5	(c) Are applications developed based on secure coding guidelines to protect applications from, at a minimum, the following vulnerabilities:					
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	□	□	□	□
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	□	□	□	□
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	□	□	□	□

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
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, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment - 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) as follows: - Is situated in front of public-facing web applications to detect and prevent web-based attacks. - Is actively running and up to date as applicable. - Is generating audit logs. - Is configured to either block web-based attacks, or generate an alert that is immediately investigated.	▪ Review documented processes ▪ Interview personnel ▪ Examine records of application security assessments ▪ Examine system configuration settings	□	□	□	□

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
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:					
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?	▪ Examine written access control policy ▪ Interview personnel ▪ Interview management ▪ Review privileged user IDs	□	□	□	□
7.1.3	Are access assigned based on individual personnel's job classification and function?	▪ Examine written access control policy ▪ Interview management ▪ Review user IDs	□	□	□	□

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
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	□	□	□	□
8.1.3	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	□	□	□	□
8.1.5	(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	□	□	□	□
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	□	□	□	□
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	□	□	□	□
8.2	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	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
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	□	□	□	□
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	□	□	□	□
8.2.4	(a) Are user passwords/passphrases changed at least once every 90 days?	▪ Review password procedures ▪ Examine system configuration settings	□	□	□	□
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	□	□	□	□
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	□	□	□	□

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
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	□	□	□	□
8.5	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	□	□	□	□
8.6	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	□	□	□	□

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
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	□	□	□	□
9.5	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	□	□	□	□
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	□	□	□	□
9.8	(a) Is all media destroyed when it is no longer needed for business or legal reasons?	▪ Review periodic media destruction policies and procedures	□	□	□	□
	(c) Is media destruction performed as follows:					

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
9.8.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	▪ Review periodic media destruction policies and procedures ▪ Interview personnel ▪ 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	□	□	□	□

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
10.2	Are automated audit trails implemented for all system components to reconstruct the following events:					
10.2.2	All actions taken by any individual with root or administrative privileges?	▪ Interview personnel ▪ Observe audit logs ▪ Examine audit log settings	□	□	□	□
10.2.4	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	□	□	□	□
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	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	**Yes with CCW**	**No**	**N/A**
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	□	□	□	□
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	□	□	□	□
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	(b) Are the following logs and security events reviewed 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 • 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 ▪ Observe processes ▪ Interview personnel	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
10.6.2	(b) Are logs of all other system components periodically reviewed—either manually or via log tools—based on the organization's policies and risk management strategy?	▪ Review security policies and procedures ▪ Review risk assessment documentation ▪ Interview personnel	□	□	□	□
10.6.3	(b) Is follow up to exceptions and anomalies identified during the review process performed?	▪ Review security policies and procedures ▪ Observe processes ▪ Interview personnel	□	□	□	□
10.7	(b) Are audit logs retained for at least one year?	▪ Review security policies and procedures ▪ Interview personnel ▪ Examine audit logs	□	□	□	□
	(c) Are at least the last three months' logs immediately available for analysis?	▪ Interview personnel ▪ Observe processes	□	□	□	□

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
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	□	□	□	□

	PCI DSS Question	Expected Testing	Response *(Check one response for each question)*				
			Yes	**Yes with CCW**	**No**	**N/A**	
11.3	***Important Note:*** *In PCI DSS version 3, the penetration testing requirements in Requirement 11.3 were expanded from the version 2 requirements. The v3 updates are best practices until June 30, 2015, after which they become requirements. Until that time, entities have the choice of validating to either the PCI DSS v2 requirements or the PCI DSS v3 requirements for penetration testing. Therefore, both sets of requirements are provided in this SAQ.* ***Instructions for completing Requirement 11.3:*** ▪ If completing this SAQ ***prior to*** July 1, 2015, answer ***either*** the PCI DSS v2 or the v3 questions for Requirement 11.3, as indicated below. ▪ If completing this SAQ ***on or after*** July 1, 2015, answer ***only*** the PCI DSS v3 questions for Requirement 11.3.						
	Complete the following: **This self-assessment for PCI DSS Requirement 11.3 was performed to (select one):**		☐ **PCI DSS v2**		☐ **PCI DSS v3**		
	*If assessing Requirement 11.3 against **PCI DSS v2**, complete the questions indicated with a "**V2**" prefix (shaded in orange).* *If assessing Requirement 11.3 against **PCI DSS v3** complete the questions indicated with a "**V3**" prefix (shaded in blue).*						
*Questions for **PCI DSS v2** Requirement 11.3 start here:*							
V2 11.3	(a) Is external penetration testing performed at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment)?	▪ Examine internal and external penetration testing results	☐	☐	☐	☐	☐
	(b) Are noted exploitable vulnerabilities corrected and testing repeated?	▪ Examine internal and external penetration testing results	☐	☐	☐	☐	☐
	(c) 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).	▪ Interview responsible personnel	☐	☐	☐	☐	☐
	(d) Do these penetration tests include the following:						
V2 11.3.1	Network-layer penetration tests? ***Note**: The tests should include components that support network functions as well as operating systems.*	▪ Examine internal and external penetration testing results	☐	☐	☐	☐	☐
V2 11.3.2	Application-layer penetration tests? ***Note**: The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.*	▪ Examine internal and external penetration testing results	☐	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*				
			Yes	Yes with CCW		No	N/A
*Questions for **PCI DSS v3** Requirement 11.3 start here:*							
V3 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 ***Note:*** *This update to Requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. Prior to this date, PCI DSS v2.0 requirements for penetration testing must be followed until version 3 is in place.*	▪ Examine penetration-testing methodology ▪ Interview responsible personnel	□	□	□	□	□
V3 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)?	▪ Interview responsible personnel	□	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*				
			Yes	Yes with CCW	No	N/A	
V3 11.3.3	Are exploitable vulnerabilities found during penetration testing corrected, followed by repeated testing to verify the corrections?	▪ Examine penetration testing results	□	□	□	□	□
V3 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 systems in the CDE?	▪ 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 systems in the CDE.	▪ Examine results from the most recent penetration test	□	□	□	□	□

	PCI DSS Question	Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
11.5	(a) Is a change-detection mechanism (for example, file-integrity monitoring tools) deployed within the cardholder data environment to detect unauthorized modification (including changes, additions, and deletions) 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	□	□	□	□
	(b) Is the change-detection mechanism configured to alert personnel to unauthorized modification (including changes, additions, and deletions) 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	□	□	□	□

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
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	□	□	□	□
12.4	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	(b) Are the following information security management responsibilities formally assigned to an individual or team:					
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	□	□	□	□
12.6	(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	□	□	□	□
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:					
12.8.1	Is a list of service providers maintained?	▪ Review policies and procedures ▪ Observe processes ▪ Review list of service providers	□	□	□	□

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
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	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
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	□	□	□	□

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

This appendix is not used for merchant assessments.

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.	

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
Example:	
3.4	Cardholder data is never stored electronically

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the SAQ A-EP 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 A-EP, 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.

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 Duly Authorized Officer of QSA Company ↑	*Date:*
Duly Authorized Officer 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.

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	□	□	

** PCI DSS Requirements indicated here refer to the questions in Section 2 of the SAQ.*