Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire C-VT and Attestation of Compliance

Merchants with Web-Based Virtual Payment Terminals – No Electronic Cardholder Data Storage

For use with PCI DSS Version 3.2

Revision 1.1
January 2017

Document Changes

Date	PCI DSS Version	SAQ Revision	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.
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*.
July 2015	3.1	1.1	Updated version numbering to align with other SAQs.
April 2016	3.2	1.0	Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2*. Requirements added from PCI DSS v3.2 Requirements 8, 9, and Appendix A2.
January 2017	3.2	1.1	Updated Document Changes to clarify requirements added in the April 2016 update. Added footnote to Before You Begin section to clarify intent of permitted systems. Added Requirement 8.3.1 to align with intent of Requirement 2.3. Added Requirement 11.3.4 to verify segmentation controls, if segmentation is used.

Table of Contents

Before You Begin

SAQ C-VT has been developed to address requirements applicable to merchants who process cardholder data only via isolated virtual payment terminals on a personal computer connected to the Internet.

A virtual payment terminal is web-browser-based access to an acquirer, processor, or third-party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.

SAQ C-VT merchants process cardholder data only via a virtual payment terminal and do not store cardholder data on any computer system. These virtual terminals are connected to the Internet to access a third party that hosts the virtual terminal payment-processing function. This third party may be a processor, acquirer, or other third-party service provider who stores, processes, and/or transmits cardholder data to authorize and/or settle merchants' virtual terminal payment transactions.

This SAQ option is intended to apply only to merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution. SAQ C-VT merchants may be brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants.

SAQ C-VT merchants confirm that, for this payment channel:

- Your company's only payment processing is via a virtual payment terminal accessed by an Internet-connected web browser;
- Your company's virtual payment terminal solution is provided and hosted by a PCI DSS validated third-party service provider;
- Your company accesses the PCI DSS-compliant virtual payment terminal solution via a computer that is isolated in a single location, and is not connected to other locations or systems within your environment (this can be achieved via a firewall or network segmentation to isolate the computer from other systems)[1];
- Your company's computer does not have software installed that causes cardholder data to be stored (for example, there is no software for batch processing or store-and-forward);
- Your company's computer does not have any attached hardware devices that are used to capture or store cardholder data (for example, there are no card readers attached);
- Your company does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the Internet);
- Any cardholder data your company retains is on paper (for example, printed reports or receipts), and these documents are not received electronically; **and**
- Your company does not store cardholder data in electronic format.

This SAQ is not applicable to e-commerce channels.

[1] This criteria is not intended to prohibit more than one of the permitted system type (that is, a virtual payment terminal accessed by an Internet-connected web browser) being on the same network zone, as long as the permitted systems are isolated from other types of systems (e.g. by implementing network segmentation). Additionally, this criteria is not intended to prevent the defined system type from being able to transmit transaction information to a third party for processing, such as an acquirer or payment processor, over a network.

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.

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 (Parts 1 & 2 of the AOC) – Assessment Information and Executive Summary.
   - Section 2 – PCI DSS Self-Assessment Questionnaire (SAQ C-VT)
   - 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 (AOC), 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

While many organizations completing SAQ C-VT will need to validate compliance with every PCI DSS requirement in this SAQ, 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 PCI DSS that are specific to managing wireless technology (for example, Requirements 1.2.3, 2.1.1, and 4.1.1).

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:		
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.*

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 (for example, retail outlets, corporate offices, data centers, call centers, etc.) included in 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	
			☐ 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 use a Qualified Integrator & Reseller (QIR)? If Yes: Name of QIR Company: QIR Individual Name: Description of services provided by QIR:	☐ Yes ☐ No
Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), 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 C-VT	
Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:	
☐	Merchant's only payment processing is via a virtual payment terminal accessed by an Internet-connected web browser;
☐	Merchant's virtual payment terminal solution is provided and hosted by a PCI DSS validated third-party service provider;
☐	Merchant accesses the PCI DSS-compliant virtual terminal solution via a computer that is isolated in a single location and is not connected to other locations or systems within the merchant environment;
☐	Merchant's computer does not have software installed that causes cardholder data to be stored (for example, there is no software for batch processing or store-and-forward);
☐	Merchant's computer does not have any attached hardware devices that are used to capture or store cardholder data (for example, there are no card readers attached);
☐	Merchant does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the Internet);
☐	Merchant does not store cardholder data in electronic format; **and**
☐	If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically.

Section 2: Self-Assessment Questionnaire C-VT

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
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	☐	☐	☐	☐
1.2.3	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	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
1.3	Is direct public access prohibited between the Internet and any system component in the cardholder data environment, as follows:					
1.3.4	Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?	▪ Examine firewall and router configurations	☐	☐	☐	☐
1.3.5	Are only established connections permitted into the network?	▪ Examine firewall and router configurations	☐	☐	☐	☐
1.4	(a) Is personal firewall software (or equivalent functionality) installed and active on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE?	▪ Review policies and configuration standards ▪ Examine mobile and/or employee-owned devices	☐	☐	☐	☐
	(b) Is the personal firewall software (or equivalent functionality) 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	☐	☐	☐	☐

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, payment applications, 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	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
	(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	☐	☐	☐	☐
2.2.2	(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	☐	☐	☐	☐
	(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? ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*	▪ 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	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
	(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	☐	☐	☐	☐
2.3	Is non-console administrative access encrypted as follows: ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*					
	(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	☐	☐	☐	☐

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	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
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 more than the first six/last four digits of the 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	☐	☐	☐	☐

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 used to safeguard sensitive cardholder data during transmission over open, public networks? ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.* *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 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	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
4.1.1	Are industry best practices used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment?	▪ Review documented standards ▪ Review wireless networks ▪ Examine system configuration settings	☐	☐	☐	☐
4.2	(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?	▪ Review policies and procedures	☐	☐	☐	☐

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	☐	☐	☐	☐

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	Is 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	☐	☐	☐	☐
8.2	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	☐	☐	☐	☐
8.2.3	(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/passphrases must have complexity and strength at least equivalent to the parameters specified above.	▪ Examine system configuration settings to verify password parameters	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
8.3	Is all individual non-console administrative access and all remote access to the CDE secured using multi-factor authentication, as follows: ***Note:*** *Multi-factor authentication requires that a minimum of 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 multi-factor authentication.*					
8.3.1	Is multi-factor authentication incorporated for all non-console access into the CDE for personnel with administrative access? ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	▪ Examine system configurations ▪ Observe administrator logging into CDE	☐	☐	☐	☐
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	☐	☐	☐	☐

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?	▪ Review periodic media destruction policies and procedures ▪ Examine security of storage containers	☐	☐	☐	☐

Regularly Monitor and Test Networks

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
11.3.4	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	☐	☐	☐	☐
	(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	☐	☐	☐	☐

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	☐	☐	☐	☐
12.3	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	☐	☐	☐	☐
12.3.3	A list of all such devices and personnel with access?	▪ Review usage policies ▪ Interview responsible personnel	☐	☐	☐	☐
12.3.5	Acceptable uses of the technologies?	▪ 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	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
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 cardholder data security policy and procedures?	▪ 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, including a description of the service(s) provided?	▪ 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	☐	☐	☐	☐

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
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	☐	☐	☐	☐
12.10.1	(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	☐	☐	☐	☐

Appendix A: Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

This appendix is not used for merchant assessments.

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
A2.1	*For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS:* • Are the devices confirmed to not be susceptible to any known exploits for SSL/early TLS *Or:* • Is there a formal Risk Mitigation and Migration Plan in place per Requirement A2.2?	▪ Review documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies POS POI devices are not susceptible to any known exploits for SSL/early TLS	☐	☐	☐	☐
A2.2	Is there a formal Risk Mitigation and Migration Plan in place for all implementations that use SSL and/or early TLS (other than as allowed in A2.1), that includes: ▪ 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 2018?	▪ Review the documented Risk Mitigation and Migration Plan	☐	☐	☐	☐

Appendix A3: Designated Entities Supplemental Validation (DESV)

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Entities required to validate to this Appendix should use the DESV Supplemental Reporting Template and Supplemental Attestation of Compliance for reporting, and consult with the applicable payment brand and/or acquirer for submission procedures.

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

This AOC is based on results noted in SAQ C-VT (Section 2), dated *(SAQ completion date).*

Based on the results documented in the SAQ C-VT noted above, 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: (***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 C-VT, 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[2], CAV2, CVC2, CID, or CVV2 data[3], or PIN data[4] 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. Qualified Security Assessor (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. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	

[2] 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.

[3] 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.

[4] 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	☐	☐	
11	Regularly test security systems and processes	☐	☐	
12	Maintain a policy that addresses information security for all personnel	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	☐	☐	

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