Payment Card Industry
Data Security Standard

Self-Assessment Questionnaire C-VT and Attestation of Compliance

For use with PCI DSS Version 4.0

Revision 1

Publication Date: December 2022

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.
June 2018	3.2.1	1.0	Updated to align with PCI DSS v3.2.1. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS Version 3.2 to 3.2.1.*
April 2022	4.0		Updated to align with PCI DSS v4.0. For details of PCI DSS changes, see PCI DSS – Summary of Changes from PCI DSS Version 3.2.1 to 4.0. Rearranged, retitled, and expanded information in the "Completing the Self-Assessment Questionnaire" section (previously titled "Before You Begin"). Aligned content in Sections 1 and 3 of Attestation of Compliance (AOC) with PCI DSS v4.0 Report on Compliance AOC. Added PCI DSS v4.0 requirements. Added appendices to support new reporting responses.
December 2022	4.0	1	Removed "In Place with Remediation" as a reporting option from Requirement Responses table, Attestation of Compliance (AOC) Part 2g, SAQ Section 2 Response column, and AOC Section 3. Also removed former Appendix C. Added "In Place with CCW" to AOC Section 3. Added guidance for responding to future-dated requirements. Added minor clarifications and addressed typographical errors.

Contents

Completing the Self-Assessment Questionnaire

Merchant Eligibility Criteria for Self-Assessment Questionnaire C-VT

Self-Assessment Questionnaire (SAQ) C-VT includes only those PCI DSS requirements applicable to merchants that process account data only via third-party virtual payment terminal solutions on an isolated computing device connected to the Internet.

A virtual payment terminal is third-party solution used to submit payment card transactions for authorization to a PCI DSS compliant third-party service provider (TPSP) website. Using this solution, the merchant manually enters account data from an isolated computing device via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card.

This SAQ option is intended to apply only to merchants that manually enter a single transaction at a time via a keyboard into an Internet-based virtual payment terminal solution. SAQ C-VT merchants may be brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants, and do not store account data on any computer system.

This SAQ is not applicable to e-commerce channels.

This SAQ is not applicable to service providers.

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

- The only payment processing is via a virtual payment terminal accessed by an Internet-connected web browser;
- The virtual payment terminal solution is provided and hosted by a PCI DSS compliant third-party service provider;
- The PCI DSS-compliant virtual payment terminal solution is only accessed via a computing device that is isolated in a single location, and is not connected to other locations or systems;
- The computing device does not have software installed that causes account data to be stored (for example, there is no software for batch processing or store-and-forward);
- The computing device does not have any attached hardware devices that are used to capture or store account data (for example, there are no card readers attached);
- The merchant does not otherwise receive, transmit, or store account data electronically through any channels (for example, via an internal network or the Internet); and
- Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically**.**

This SAQ includes only those requirements that apply to a specific type of merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to the cardholder data environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for the merchant's environment.

Defining Account Data, Cardholder Data, and Sensitive Authentication Data

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

Refer to PCI DSS Section 2, *PCI DSS Applicability Information*, for further details.

PCI DSS Self-Assessment Completion Steps

1. Confirm by review of the eligibility criteria in this SAQ and the *Self-Assessment Questionnaire Instructions and Guidelines* document on the PCI SSC website that this is the correct SAQ for the merchant's environment.
2. Confirm that the merchant environment is properly scoped.
3. Assess the environment for compliance with PCI DSS requirements.
4. Complete all sections of this document:
   - Section 1: Assessment Information (Parts 1 & 2 of the Attestation of Compliance (AOC) – Contact Information and Executive Summary).
   - Section 2: Self-Assessment Questionnaire C-VT.
   - Section 3: Validation and Attestation Details (Parts 3 & 4 of the AOC – PCI DSS Validation and Action Plan for Non-Compliant Requirements (if Part 4 is applicable)).
5. Submit the SAQ and AOC, along with any other requested documentation—such as ASV scan reports—to the requesting organization (those organizations that manage compliance programs such as payment brands and acquirers).

Expected Testing

The instructions provided in the "Expected Testing" column are based on the testing procedures in PCI DSS and provide a high-level description of the types of testing activities that a merchant is expected to perform to verify that a requirement has been met.

The intent behind each testing method is described as follows:

- Examine: The merchant critically evaluates data evidence. Common examples include documents (electronic or physical), screenshots, configuration files, audit logs, and data files.
- Observe: The merchant watches an action or views something in the environment. Examples of observation subjects include personnel performing a task or process, system components performing a function or responding to input, environmental conditions, and physical controls.

- Interview: The merchant converses with individual personnel. Interview objectives may include confirmation of whether an activity is performed, descriptions of how an activity is performed, and whether personnel have particular knowledge or understanding.

The testing methods are intended to allow the merchant to demonstrate how it has met a requirement. The specific items to be examined or observed and personnel to be interviewed should be appropriate for both the requirement being assessed and the merchant's particular implementation.

Full details of testing procedures for each requirement can be found in PCI DSS.

Requirement Responses

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

A description of the meaning for each response and when to use each response is provided in the table below:

Response	When to use this response:
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated.
In Place with CCW (Compensating Controls 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 Controls Worksheet (CCW) in Appendix B of this SAQ. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in PCI DSS in Appendices B and C.
Not Applicable	The requirement does not apply to the merchant's environment. (See "Guidance for Not Applicable Requirements" below for examples.) All responses in this column require a supporting explanation in Appendix C of this SAQ.
Not Tested	*This response is not applicable to, and not included as an option for, this SAQ.* *This SAQ was created for a specific type of environment based on how the merchant stores, processes, and/or transmits account data and defines the specific PCI DSS requirements that apply for this environment. Consequently, all requirements in this SAQ must be tested.*
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before the merchant can confirm they are in place. Responses in this column may require the completion of Part 4, if requested by the entity to which this SAQ will be submitted. This response is also used if a requirement cannot be met due to a legal restriction. (See "Legal Exception" below for more guidance).

Guidance for Not Applicable Requirements

If any requirements do not apply to the merchant's environment, select the Not Applicable option for that specific requirement. For example, in this SAQ, requirements for securing all media with cardholder data (Requirements 9.4.1 - 9.4.6) only apply if a merchant stores paper media with cardholder data; if paper media is not stored, the merchant can select Not Applicable for those requirements.

For each response where Not Applicable is selected in this SAQ, complete *Appendix C: Explanation of Requirements Noted as Not Applicable*.

Guidance for Responding to Future Dated Requirements

In Section 2 below, each new PCI DSS v4.0 requirement or bullet with an extended implementation period includes the following note: "*This requirement [or bullet] is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment*."

These new requirements are not required to be included in a PCI DSS assessment until the future date has passed. Prior to that future date, any new requirements with an extended implementation date that have not been implemented by the merchant may be marked as Not Applicable and documented in *Appendix C: Explanation of Requirements Noted as Not Applicable*.

Legal Exception

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS requirement, select Not in Place for that requirement and complete the relevant attestation in Section 3, Part 3 of this SAQ.

Note: *A legal restriction is one where meeting the PCI DSS requirement would violate a local or regional law or regulation.*

Contractual obligations or legal advice are not legal restrictions.

Use of the Customized Approach

SAQs cannot be used to document use of the Customized Approach to meet PCI DSS requirements. For this reason, the Customized Approach Objectives are not included in SAQs. Entities wishing to validate using the Customized Approach may be able to use the PCI DSS Report on Compliance (ROC) Template to document the results of their assessment.

Use of the Customized Approach is not supported in SAQs.

The use of the customized approach may be regulated by organizations that manage compliance programs, such as payment brands and acquirers. Questions about use of a customized approach should always be referred to those organizations. This includes whether an entity that is eligible for an SAQ may instead complete a ROC to use a customized approach, and whether an entity is required to use a QSA, or may use an ISA, to complete an assessment using the customized approach. Information about the use of the Customized Approach can be found in Appendices D and E of PCI DSS.

Additional PCI SSC Resources

Additional resources that provide guidance on PCI DSS requirements and how to complete the self-assessment questionnaire have been provided below to assist with the assessment process.

Resource	Includes:
PCI DSS *(PCI Data Security Standard Requirements and Testing Procedures)*	▪ Guidance on Scoping ▪ Guidance on the intent of all PCI DSS Requirements ▪ Details of testing procedures ▪ Guidance on Compensating Controls ▪ Appendix G: Glossary of Terms, Abbreviations, and Acronyms
SAQ Instructions and Guidelines	▪ Information about all SAQs and their eligibility criteria ▪ How to determine which SAQ is right for your organization
Frequently Asked Questions (FAQs)	▪ Guidance and information about SAQs.
Online PCI DSS Glossary	▪ PCI DSS Terms, Abbreviations, and Acronyms
Information Supplements and Guidelines	▪ Guidance on a variety of PCI DSS topics including: – *Understanding PCI DSS Scoping and Network Segmentation* – *Third-Party Security Assurance* – *Multi-Factor Authentication Guidance* – *Best Practices for Maintaining PCI DSS Compliance*
Getting Started with PCI	▪ Resources for smaller merchants including: – *Guide to Safe Payments* – *Common Payment Systems* – *Questions to Ask Your Vendors* – *Glossary of Payment and Information Security Terms* – *PCI Firewall Basics*

These and other resources can be found on the PCI SSC website *(www.pcisecuritystandards.org)*.

Organizations are encouraged to review PCI DSS and other supporting documents before beginning an assessment.

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures.* Complete all sections. The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which the Attestation of Compliance (AOC) will be submitted for reporting and submission procedures.

Part 1. Contact Information	
Part 1a. Assessed Merchant	
Company name:	
DBA (doing business as):	
Company mailing address:	
Company main website:	
Company contact name:	
Company contact title:	
Contact phone number:	
Contact e-mail address:	
Part 1b. Assessor	
Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	
Qualified Security Assessor	
Company name:	
Company mailing address:	
Company website:	
Lead Assessor name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	

Part 2. Executive Summary

Part 2a. Merchant Business Payment Channels (select all that apply):

Indicate all payment channels used by the business that are included in this assessment.

☐ Mail order/telephone order (MOTO)

☐ E-Commerce

☐ Card-present

Are any payment channels not included in this assessment? If yes, indicate which channel(s) is not included in the assessment and provide a brief explanation about why the channel was excluded.	☐ Yes ☐ No

Note: *If the organization has a payment channel that is not covered by this SAQ, consult with the entity(ies) to which this AOC will be submitted about validation for the other channels.*

Part 2b. Description of Role with Payment Cards

For each payment channel included in this assessment as selected in Part 2a above, describe how the business stores, processes and/or transmits account data.

Channel	How Business Stores, Processes, and/or Transmits Account Data

Part 2c. Description of Payment Card 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 POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	
Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)*	☐ Yes ☐ No

Part 2. Executive Summary *(continued)*

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities (for example, retail locations, corporate offices, data centers, call centers, and mail rooms) in scope for the PCI DSS assessment.

Facility Type	Total number of locations (How many locations of this type are in scope)	Location(s) of facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*

Part 2e. PCI SSC Validated Products and Solutions

Does the merchant use any item identified on any PCI SSC Lists of Validated Products and Solutions♦?

☐ Yes ☐ No

Provide the following information regarding each item the merchant uses from PCI SSC's Lists of Validated Products and Solutions.

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing (YYYY-MM-DD)
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD

♦ For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers

Does the merchant have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the merchant's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)	☐ Yes ☐ No
• Manage system components included in the scope of the merchant's PCI DSS assessment—for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers.	☐ Yes ☐ No
• Could impact the security of the merchant's CDE (for example, vendors providing support via remote access, and/or bespoke software developers)	☐ Yes ☐ No

If Yes:

Name of service provider:	**Description of service(s) provided:**

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

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment

(SAQ Section 2 and related appendices)

Indicate below all responses that were selected for each PCI DSS requirement.

PCI DSS Requirement *	Requirement Responses *More than one response may be selected for a given requirement. Indicate all responses that apply.*			
	In Place	In Place with CCW	Not Applicable	Not in Place
Requirement 1:	☐	☐	☐	☐
Requirement 2:	☐	☐	☐	☐
Requirement 3:	☐	☐	☐	☐
Requirement 4:	☐	☐	☐	☐
Requirement 5:	☐	☐	☐	☐
Requirement 6:	☐	☐	☐	☐
Requirement 7:	☐	☐	☐	☐
Requirement 8:	☐	☐	☐	☐
Requirement 9:	☐	☐	☐	☐
Requirement 12:	☐	☐	☐	☐

** PCI DSS Requirements indicated above refer to the requirements in Section 2 of this SAQ.*

Part 2. Executive Summary *(continued)*

Part 2h. Eligibility to Complete SAQ C-VT

Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment channel:

☐	The only payment processing is via a virtual payment terminal accessed by an Internet-connected web browser.
☐	The virtual payment terminal solution is provided and hosted by a PCI DSS validated third-party service provider.
☐	The PCI DSS-compliant virtual payment terminal solution is only accessed via a computing device that is isolated in a single location and is not connected to other locations or systems.
☐	The computing device does not have software installed that causes account data to be stored (for example, there is no software for batch processing or store-and-forward).
☐	The computing device does not have any attached hardware devices that are used to capture or store account data (for example, there are no card readers attached).
☐	The merchant does not otherwise receive, transmit, or store account data electronically through any channels (for example, via an internal network or the Internet).
☐	Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Section 2: Self-Assessment Questionnaire C-VT

Note: *The following requirements mirror the requirements in the* PCI DSS Requirements and Testing Procedures *document.*

Self-assessment completion date: YYYY-MM-DD

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain network security controls

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*			
			In Place	In Place with CCW	Not Applicable	Not in Place
1.3 Network access to and from the cardholder data environment is restricted.						
1.3.1	Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary, • All other traffic is specifically denied.	• Examine NSC configuration standards. • Examine NSC configurations.	☐	☐	☐	☐
1.3.2	Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	• Examine NSC configuration standards. • Examine NSC configurations.	☐	☐	☐	☐
1.3.3	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.	• Examine configuration settings. • Examine network diagrams.	☐	☐	☐	☐

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.						
1.5.1	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: ▪ Specific configuration settings are defined to prevent threats being introduced into the entity's network. ▪ Security controls are actively running. ▪ Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	• Examine policies and configuration standards. • Examine device configuration settings.	☐	☐	☐	☐
	Applicability Notes These security controls may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If these security controls need to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which these security controls are not active. This requirement applies to employee-owned and company-owned computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit.					

Requirement 2: Apply Secure Configurations to All System Components

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.						
2.1.1	All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☐	☐	☐	☐
2.2 System components are configured and managed securely.						
2.2.2	Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.	• Examine system configuration standards. • Examine vendor documentation. • Observe a system administrator logging on using vendor default accounts. • Examine configuration files. • Interview personnel.	☐	☐	☐	☐
	Applicability Notes This applies to ALL vendor default accounts and 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, and Simple Network Management Protocol (SNMP) defaults. This requirement also applies where a system component is not installed within an entity's environment, for example, software and applications that are part of the CDE and are accessed via a cloud subscription service.					
2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	• Examine system configuration standards. • Examine system configurations.	☐	☐	☐	☐

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
2.2.5	If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	• Examine configuration standards. • Interview personnel. • Examine configuration settings.	☐	☐	☐	☐
2.2.6	System security parameters are configured to prevent misuse.	• Examine system configuration standards. • Interview personnel. • Examine system configurations.	☐	☐	☐	☐
2.2.7	All non-console administrative access is encrypted using strong cryptography.	• Examine system configuration standards. • Observe an administrator log on. • Examine system configurations. • Examine vendor documentation. • Interview personnel.	☐	☐	☐	☐
	Applicability Notes This includes administrative access via browser-based interfaces and application programming interfaces (APIs).					

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
2.3 Wireless environments are configured and managed securely.						
2.3.1	For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults.	• Examine policies and procedures. • Review vendor documentation. • Examine wireless configuration settings. • Interview personnel.	☐	☐	☐	☐
	Applicability Notes This includes, but is not limited to, default wireless encryption keys, passwords on wireless access points, SNMP defaults, and any other security-related wireless vendor defaults.					
2.3.2	For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. • Whenever a key is suspected of or known to be compromised.	• Examine key-management documentation. • Interview personnel.	☐	☐	☐	☐

Protect Account Data

Requirement 3: Protect Stored Account Data

Note: *For SAQ C-VT, Requirement 3 applies only to merchants with paper records that include account data (for example, receipts or printed reports).*

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*			
			In Place	In Place with CCW	Not Applicable	Not in Place
3.1 Processes and mechanisms for protecting stored account data are defined and understood.						
3.1.1	All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☐	☐	☐	☐
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 3.1.1 means that, if the merchant has paper storage of account data, the merchant has policies and procedures in place that govern merchant activities for Requirement 3. This helps to ensure personnel are aware of and following security policies and documented operational procedures for managing the secure storage of any paper records with account data.* *If merchant does not store paper records with account data, mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.*						

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
3.3 Sensitive authentication data (SAD) is not stored after authorization.						
3.3.1	SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	• Examine documented policies and procedures. • Examine system configurations. • Observe the secure data deletion processes.	☐	☐	☐	☐
	Applicability Notes *Part of this Applicability Note is intentionally removed for this SAQ as does not apply to merchant assessments.* Sensitive authentication data includes the data cited in Requirement 3.3.1.2.					
3.3.1.2	The card verification code is not retained upon completion of the authorization process.	• Examine data sources.	☐	☐	☐	☐
	Applicability Notes The card verification code is the three- or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions.					

SAQ Completion Guidance:

Selection of any of the In Place responses for Requirement 3.3.1.2 means that if the merchant writes down the card verification code while a transaction is being conducted, the merchant either securely destroys the paper (for example, with a shredder) immediately after the transaction is complete, or obscures the code (for example, by "blacking it out" with a marker) before the paper is stored.

If the merchant never requests the three-digit or four-digit number printed on the front or back of a payment card ("card verification code"), the merchant marks the Not Applicable column and completes Appendix C: Explanation of Requirements Noted as Not Applicable.

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
3.4 Access to displays of full PAN and ability to copy PAN is restricted.						
3.4.1	PAN is masked when displayed (the BIN 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 BIN and last four digits of the PAN.	• Examine documented policies and procedures. • Examine system configurations. • Examine the documented list of roles that need access to more than the BIN and last four digits of the PAN (includes full PAN). • Examine displays of PAN (for example, on screen, on paper receipts).	☐	☐	☐	☐
	Applicability Notes This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment brand requirements for point-of-sale (POS) receipts. This requirement relates to protection of PAN where it is displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.5.1 for protection of PAN when stored, processed, or transmitted.					

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
4.2 PAN is protected with strong cryptography during transmission.						
4.2.1.2	Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	• Examine system configurations.	☐	☐	☐	☐

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

Maintain a Vulnerability Management Program

Requirement 5: Protect All Systems and Networks from Malicious Software

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
5.2 Malicious software (malware) is prevented, or detected and addressed.						
5.2.1	An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	• Examine system components. • Examine the periodic evaluations.	☐	☐	☐	☐
5.2.2	The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	• Examine vendor documentation. • Examine system configurations.	☐	☐	☐	☐
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.						
5.3.1	The anti-malware solution(s) is kept current via automatic updates.	• Examine anti-malware solution(s) configurations, including any master installation. • Examine system components and logs.	☐	☐	☐	☐
5.3.2	The anti-malware solution(s): • Performs periodic scans and active or real-time scans, **OR** • Performs continuous behavioral analysis of systems or processes.	• Examine anti-malware solution(s) configurations, including any master installation. • Examine system components. • Examine logs and scan results.	☐	☐	☐	☐

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
5.3.3	For removable electronic media, the anti-malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, **OR** • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.	• Examine anti-malware solution(s) configurations. • Examine system components with removable electronic media. • Examine logs and scan results.	☐	☐	☐	☐
	Applicability Notes *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*					
5.3.4	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	• Examine anti-malware solution(s) configurations.	☐	☐	☐	☐
5.3.5	Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	• Examine anti-malware configurations. • Observe processes. • Interview responsible personnel.	☐	☐	☐	☐
	Applicability Notes Anti-malware solutions may be temporarily disabled only if there is a legitimate technical need, as authorized by management on a case-by-case basis. If anti-malware 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 during which anti-malware protection is not active.					

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
5.4 Anti-phishing mechanisms protect users against phishing attacks.						
5.4.1	Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.	• Observe implemented processes. • Examine mechanisms.	☐	☐	☐	☐
	Applicability Notes This requirement applies to the automated mechanism. It is not intended that the systems and services providing such automated mechanisms (such as e-mail servers) are brought into scope for PCI DSS. The focus of this requirement is on protecting personnel with access to system components in-scope for PCI DSS. Meeting this requirement for technical and automated controls to detect and protect personnel against phishing is not the same as Requirement 12.6.3.1 for security awareness training. Meeting this requirement does not also meet the requirement for providing personnel with security awareness training, and vice versa. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*					

Requirement 6: Develop and Maintain Secure Systems and Software

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
6.3 Security vulnerabilities are identified and addressed.						
6.3.1	Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • *Bullet intentionally left blank for this SAQ.* .	• Examine policies and procedures. • Interview responsible personnel. • Examine documentation. • Observe processes.	☐	☐	☐	☐
	Applicability Notes This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.					
6.3.3	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • *Bullet intentionally left blank for this SAQ.*	• Examine policies and procedures. • Examine system components and related software. • Compare list of security patches installed to recent vendor patch lists.	☐	☐	☐	☐

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

Implement Strong Access Control Measures

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*			
			In Place	In Place with CCW	Not Applicable	Not in Place
7.2 Access to system components and data is appropriately defined and assigned.						
7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.	• Examine policies and procedures. • Examine user access settings, including for privileged users. • Interview responsible management personnel. • Interview personnel responsible for assigning access.	☐	☐	☐	☐

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

Requirement 8: Identify Users and Authenticate Access to System Components

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.						
8.1.1	All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☐	☐	☐	☐
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 8.1.1 means that the merchant has policies and procedures in place that govern merchant activities for Requirement 8.*						
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.						
8.2.1	All users are assigned a unique ID before access to system components or cardholder data is allowed.	• Interview responsible personnel. • Examine audit logs and other evidence.	☐	☐	☐	☐
	Applicability Notes This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).					

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
8.2.2	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.	• Examine user account lists on system components and applicable documentation. • Examine authentication policies and procedures. • Interview system administrators.	☐	☐	☐	☐
	Applicability Notes This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).					
8.2.4	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified on the documented approval.	• Examine documented authorizations across various phases of the account lifecycle (additions, modifications, and deletions). • Examine system settings.	☐	☐	☐	☐
	Applicability Notes This requirement applies to all user accounts, including employees, contractors, consultants, temporary workers, and third-party vendors.					

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
8.2.5	Access for terminated users is immediately revoked.	• Examine information sources for terminated users. • Review current user access lists. • Interview responsible personnel.	☐	☐	☐	☐
8.3 Strong authentication for users and administrators is established and managed.						
8.3.1	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • 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 element.	• Examine documentation describing the authentication factor(s) used. • For each type of authentication factor used with each type of system component, observe the authentication process.	☐	☐	☐	☐
	Applicability Notes This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement does not supersede multi-factor authentication (MFA) requirements but applies to those in-scope systems not otherwise subject to MFA requirements. A digital certificate is a valid option for "something you have" if it is unique for a particular user.					

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
8.3.6	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters.	• Examine system configuration settings.	☐	☐	☐	☐
	Applicability Notes This requirement is not intended to apply to: ▪ User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). ▪ Application or system accounts, which are governed by requirements in section 8.6. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.					
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.						
8.4.1	MFA is implemented for all non-console access into the CDE for personnel with administrative access.	• Examine network and/or system configurations. • Observe administrator personnel logging into the CDE.	☐	☐	☐	☐
	Applicability Notes The requirement for MFA for non-console administrative access applies to all personnel with elevated or increased privileges accessing the CDE via a non-console connection—that is, via logical access occurring over a network interface rather than via a direct, physical connection. MFA is considered a best practice for non-console administrative access to in-scope system components that are not part of the CDE.					

Requirement 9: Restrict Physical Access to Cardholder Data

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.						
9.1.1	All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☐	☐	☐	☐
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 9.1.1 means that the merchant has policies and procedures in place that govern merchant activities for Requirement 9, including how any paper media with cardholder data is secured, and how POI devices are protected.*						
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.						
9.2.1	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	• Observe physical entry controls. • Interview responsible personnel.	☐	☐	☐	☐
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.						
Note: *For SAQ C-VT, Requirements at 9.4 only apply to merchants with paper records (for example, receipts or printed reports) with account data, including primary account numbers (PANs).*						
9.4.1	All media with cardholder data is physically secured.	• Examine documentation.	☐	☐	☐	☐
9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	• Examine documented procedures. • Examine logs or other documentation. • Interview responsible personnel at the storge location(s).	☐	☐	☐	☐
9.4.2	All media with cardholder data is classified in accordance with the sensitivity of the data.	• Examine documented procedures. • Examine media logs or other documentation.	☐	☐	☐	☐

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
9.4.3	Media with cardholder data sent outside the facility is secured as follows: • *Bullet intentionally left blank for this SAQ.* • Media is sent by secured courier or other delivery method that can be accurately tracked. • *Bullet intentionally left blank for this SAQ.*	• Examine documented procedures. • Interview personnel. • Examine records. • Examine offsite tracking logs for all media.	☐	☐	☐	☐
9.4.4	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	• Examine documented procedures. • Examine offsite media tracking logs. • Interview responsible personnel.	☐	☐	☐	☐
	Applicability Notes Individuals approving media movements should have the appropriate level of management authority to grant this approval. However, it is not specifically required that such individuals have "manager" as part of their title.					
9.4.6	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.	• Examine the periodic media destruction policy. • Observe processes. • Interview personnel. • Observe storage containers.	☐	☐	☐	☐
	Applicability Notes These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.					

SAQ Completion Guidance:

Selection of any of the In Place responses for Requirements at 9.4 means that the merchant securely stores any paper media with account data, for example by storing the paper in a locked drawer, cabinet, or safe, and that the merchant destroys such paper when no longer needed for business purposes. This includes a written document or policy for employees, so they know how to secure paper with account data and how to destroy the paper when no longer needed.

Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs

Note: *Requirement 12 specifies that merchants have information security policies for their personnel, but these policies can be as simple or complex as needed for the size and complexity of the merchant's operations. The policy document must be provided to all personnel so they are aware of their responsibilities for protecting payment terminals, any paper documents with account data, etc. If a merchant has no employees, then it is expected that the merchant understands and acknowledges their responsibility for security within their store(s).*

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.						
12.1.1	An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	• Examine the information security policy. • Interview personnel.	☐	☐	☐	☐
12.1.2	The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment	• Examine the information security policy. • Interview responsible personnel.	☐	☐	☐	☐
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirements 12.1.1 and 12.1.2 means that the merchant has a security policy that is reasonable for the size and complexity of the merchant's operations, and that the policy is reviewed at least once every 12 months and updated if needed.*						

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.6 Security awareness education is an ongoing activity.						
12.6.1	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	• Examine the security awareness program.	☐	☐	☐	☐
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 12.6.1 means that the merchant has a security awareness program in place, consistent with the size and complexity of the merchant's operations. For example, a simple awareness program could be a flyer posted in the back office, or a periodic e-mail sent to all employees. Examples of awareness program messaging include descriptions of security tips all employees should follow, such as how to lock doors and storage containers, how to determine whether a payment terminal has been tampered with, and processes to confirm the identify and verify there is a legitimate business reason for any service workers when they arrive to service payment terminals.*						
12.6.3.1	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: • Phishing and related attacks. • Social engineering.	• Examine security awareness training content.	☐	☐	☐	☐
	Applicability Notes See Requirement 5.4.1 in PCI DSS for guidance on the difference between technical and automated controls to detect and protect users from phishing attacks, and this requirement for providing users security awareness training about phishing and social engineering. These are two separate and distinct requirements, and one is not met by implementing controls required by the other one. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*					

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.						
12.8.1	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	• Examine policies and procedures. • Examine list of TPSPs.	☐	☐	☐	☐
	Applicability Notes					
	The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.					
12.8.2	Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	• Examine policies and procedures. • Examine written agreements with TPSPs.	☐	☐	☐	☐
	Applicability Notes					
	The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgment does not have to include the exact wording provided in this requirement. Evidence that a TPSP is meeting PCI DSS requirements (for example, a PCI DSS Attestation of Compliance (AOC) or a declaration on a company's website) is not the same as a written agreement specified in this requirement.					

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
12.8.3	An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	• Examine policies and procedures. • Examine evidence. • Interview responsible personnel.	☐	☐	☐	☐
12.8.4	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	☐	☐	☐	☐
	Applicability Notes Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for example, via a firewall service), the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also "not in place" for the entity.					
12.8.5	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	☐	☐	☐	☐
SAQ Completion Guidance: *Selection of any of the In Place responses for requirements at 12.8.1 through 12.8.4 means that the merchant has a list of, and agreements with, service providers they share account data with or that could impact the security of the merchant's cardholder data environment. For example, such agreements would be applicable if a merchant uses a document-retention company to store paper documents that include account data or if a merchant's vendor accesses merchant systems remotely to perform maintenance.*						
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.						
12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident.	• Examine the incident response plan. • Interview personnel. • Examine documentation from previously reported incidents.	☐	☐	☐	☐
SAQ Completion Guidance: *Selection of any of the In Place responses for Requirement 12.10.1 means that the merchant has documented an incident response and escalation plan to be used for emergencies, consistent with the size and complexity of the merchant's operations. For example, such a plan could be a simple document posted in the back office that lists who to call in the event of various situations with an annual review to confirm it is still accurate, but could extend all the way to a full incident response plan including backup "hotsite" facilities and thorough annual testing. This plan should be readily available to all personnel as a resource in an emergency.*						

Appendix A: Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers

This Appendix is not used for merchant assessments.

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections

This Appendix is not used for SAQ C-VT merchant assessments.

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

This Appendix must be completed to define compensating controls for any requirement where In Place with CCW was selected.

Note: *Only entities that have a legitimate and documented technological or business constraint can consider the use of compensating controls to achieve compliance.*

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

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	Document the legitimate technical or business constraints precluding compliance with the original requirement.	
2. Definition of Compensating Controls	Define the compensating controls: explain how they address the objectives of the original control and the increased risk, if any.	
3. Objective	Define the objective of the original control.	
	Identify the objective met by the compensating control. ***Note:*** *This can be, but is not required to be, the stated Customized Approach Objective listed for this requirement in PCI DSS.*	
4. Identified Risk	Identify any additional risk posed by the lack of the original control.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process(es) and controls in place to maintain compensating controls.	

Appendix C: Explanation of Requirements Noted as Not Applicable

This Appendix must be completed for each requirement where Not Applicable was selected.

Requirement	Reason Requirement is Not Applicable
Example:	
Requirement 3.5.1	*Account data is never stored electronically*

Appendix D: Explanation of Requirements Noted as Not Tested

This Appendix is not used for SAQ C-VT merchant assessments.

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 (Self-assessment completion date *YYYY-MM-DD).*

Based on the results documented in the SAQ C-VT noted above, each signatory identified in any of Parts 3b–3d, as applicable, assert(s) the following compliance status for the merchant identified in Part 2 of this document.

Select one:

☐	**Compliant:** All sections of the PCI DSS SAQ are complete and all requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *(Merchant Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Merchant Company Name)* has not demonstrated compliance with the PCI DSS requirements included in this SAQ. **Target Date** for Compliance: *YYYY-MM-DD* A merchant submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted *before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements in the PCI DSS SAQ are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Merchant Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3a. Merchant Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☐	PCI DSS Self-Assessment Questionnaire C-VT, Version *4.0* was completed according to the instructions therein.
☐	All information within the above-referenced SAQ and in this attestation fairly represents the results of the merchant's assessment in all material respects.
☐	PCI DSS controls will be maintained at all times, as applicable to the merchant's environment.

Part 3b. Merchant Attestation

Signature of Merchant Executive Officer ↑	*Date: YYYY-MM-DD*
Merchant Executive Officer Name:	*Title:*

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this assessment, indicate the role performed:	☐ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Signature of Lead QSA ↑	*Date: YYYY-MM-DD*
Lead QSA Name:	

Signature of Duly Authorized Officer of QSA Company ↑	*Date: YYYY-MM-DD*
Duly Authorized Officer Name:	*QSA Company:*

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has a Non-Compliant status noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the merchant expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

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 network security controls	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	

** PCI DSS Requirements indicated above refer to the requirements in Section 2 of this SAQ.*