



Payment Card Industry Data Security Standard

Self-Assessment Questionnaire C and Attestation of Compliance

For use with PCI DSS Version 4.0.1

Publication Date: October 2024

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 <i>PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1</i> .
July 2015	3.1	1.1	Updated to remove references to “best practices” prior to June 30, 2015.
April 2016	3.2	1.0	Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see <i>PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2</i> . 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. Checkboxes fixed in Requirements 8.1.6 and 11.3.4.
June 2018	3.2.1	1.0	Updated to align with PCI DSS v3.2.1. For details of PCI DSS changes, see <i>PCI DSS – Summary of Changes from PCI DSS Version 3.2 to 3.2.1</i> .
April 2022	4.0		Updated to align with PCI DSS v4.0. For details of PCI DSS changes, see <i>PCI DSS – Summary of Changes from PCI DSS Version 3.2.1 to 4.0</i> . 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.
October 2024	4.0.1		Updated to align with PCI DSS v4.0.1. For details of PCI DSS changes, see <i>PCI DSS Summary of Changes from PCI DSS Version 4.0 to 4.0.1</i> . Added ASV Resource Guide to section “Additional PCI SSC Resources.” Deleted Requirement 10.3.3 added in v4.0 of this SAQ, because the requirement is not relevant for SAQ C merchants.

Contents

Document Changes	ii
Completing the Self-Assessment Questionnaire	iv
Merchant Eligibility Criteria for Self-Assessment Questionnaire C	iv
Defining Account Data, Cardholder Data, and Sensitive Authentication Data	iv
PCI DSS Self-Assessment Completion Steps	v
Expected Testing	v
Requirement Responses	v
Additional PCI SSC Resources	viii
Section 1: Assessment Information	1
Section 2: Self-Assessment Questionnaire C	7
Build and Maintain a Secure Network and Systems	7
<i>Requirement 1: Install and Maintain Network Security Controls</i>	<i>7</i>
<i>Requirement 2: Apply Secure Configurations to All System Components</i>	<i>8</i>
Protect Account Data	12
<i>Requirement 3: Protect Stored Account Data</i>	<i>12</i>
<i>Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks</i>	<i>15</i>
Maintain a Vulnerability Management Program	17
<i>Requirement 5: Protect All Systems and Networks from Malicious Software</i>	<i>17</i>
<i>Requirement 6: Develop and Maintain Secure Systems and Software</i>	<i>21</i>
Implement Strong Access Control Measures	26
<i>Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know</i>	<i>26</i>
<i>Requirement 8: Identify Users and Authenticate Access to System Components</i>	<i>28</i>
<i>Requirement 9: Restrict Physical Access to Cardholder Data</i>	<i>40</i>
Regularly Monitor and Test Networks	45
<i>Requirement 10: Log and Monitor All Access to System Components and Cardholder Data</i>	<i>45</i>
<i>Requirement 11: Test Security of Systems and Networks Regularly</i>	<i>50</i>
Maintain an Information Security Policy	55
<i>Requirement 12: Support Information Security with Organizational Policies and Programs</i>	<i>55</i>
Appendix A: Additional PCI DSS Requirements	62
<i>Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers</i>	<i>62</i>
<i>Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections</i>	<i>62</i>
<i>Appendix A3: Designated Entities Supplemental Validation (DESV)</i>	<i>63</i>
Appendix B: Compensating Controls Worksheet	64
Appendix C: Explanation of Requirements Noted as Not Applicable	65
Appendix D: Explanation of Requirements Noted as Not Tested	66
Section 3: Validation and Attestation Details	67

Completing the Self-Assessment Questionnaire

Merchant Eligibility Criteria for Self-Assessment Questionnaire C

Self-Assessment Questionnaire (SAQ) C includes only those PCI DSS requirements applicable to merchants with payment application systems (for example, point-of-sale systems) connected to the Internet, and that do not store electronic account data.

SAQ C merchants process account data via a point-of-sale (POS) system or other payment application systems connected to the Internet, do not store account data on any computer system, and may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants.

This SAQ is not applicable to e-commerce channels.

This SAQ is not applicable to service providers.

SAQ C merchants confirm that, for this payment channel:

- The merchant has a payment application system and an Internet connection on the same device and/or same local area network (LAN);
- The payment application system is not connected to any other systems within the merchant environment (this can be achieved via network segmentation to isolate payment application system/Internet device from all other systems);
- The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single store only;
- The merchant does not store account data in electronic format, 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 cardholder data and/or sensitive authentication data. Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Account Data	
Cardholder Data includes:	Sensitive Authentication Data includes:
<ul style="list-style-type: none"> • Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code 	<ul style="list-style-type: none"> • 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.
 - 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 entity'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)	<p>The expected testing has been performed, and the requirement has been met with the assistance of a compensating control.</p> <p>All responses in this column require completion of a Compensating Controls Worksheet (CCW) in Appendix B of this SAQ.</p> <p>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.</p>
Not Applicable	<p>The requirement does not apply to the entity's environment. (See "Guidance for Not Applicable Requirements" below for examples.)</p> <p>All responses in this column require a supporting explanation in Appendix C of this SAQ.</p>
Not Tested	<p><i>This response is not applicable to, and not included as an option for, this SAQ.</i></p> <p><i>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.</i></p>
Not in Place	<p>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.</p> <p>This response is also used if a requirement cannot be met due to a legal restriction. (See "Legal Exception" below for more guidance).</p>

Guidance for Not Applicable Requirements

If any requirements do not apply to the entity'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 PCI DSS 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 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 exception is a legal restriction due to a local or regional law, regulation, or regulatory requirement, where meeting a PCI DSS requirement would violate that law, regulation, or regulatory requirement.

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 Data Security Standard Requirements and Testing Procedures (PCI DSS)	<ul style="list-style-type: none"> ▪ 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	<ul style="list-style-type: none"> ▪ Information about all SAQs and their eligibility criteria ▪ How to determine which SAQ is right for your organization
Frequently Asked Questions (FAQs)	<ul style="list-style-type: none"> ▪ Guidance and information about SAQs.
Online PCI DSS Glossary	<ul style="list-style-type: none"> ▪ PCI DSS Terms, Abbreviations, and Acronyms
Information Supplements and Guidelines	<ul style="list-style-type: none"> ▪ Guidance on a variety of PCI DSS topics including: <ul style="list-style-type: none"> – <i>Understanding PCI DSS Scoping and Network Segmentation</i> – <i>Third-Party Security Assurance</i> – <i>Multi-Factor Authentication Guidance</i> – <i>Best Practices for Maintaining PCI DSS Compliance</i>
Getting Started with PCI	<ul style="list-style-type: none"> ▪ Resources for smaller merchants including: <ul style="list-style-type: none"> – <i>Guide to Safe Payments</i> – <i>Common Payment Systems</i> – <i>Questions to Ask Your Vendors</i> – <i>Glossary of Payment and Information Security Terms</i> – <i>PCI Firewall Basics</i> – <i>ASV Resource Guide</i>

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

<p>Are any payment channels not included in this assessment?</p> <p>If yes, indicate which channel(s) is not included in the assessment and provide a brief explanation about why the channel was excluded.</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
---	---

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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>

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, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions, and Mobile Payments on COTS (MPoC) products.

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			
	<i>More than one response may be selected for a given requirement. Indicate all responses that apply.</i>			
	In Place	In Place with CCW	Not Applicable	Not in Place
Requirement 1:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

** 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

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

<input type="checkbox"/>	The merchant has a payment application system and an Internet connection on the same device and/or same local area network (LAN).
<input type="checkbox"/>	The payment application system is not connected to any other system within the merchant environment.
<input type="checkbox"/>	The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single location only.
<input type="checkbox"/>	Merchant does not store account data in electronic format.
<input type="checkbox"/>	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

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: <ul style="list-style-type: none"> To only traffic that is necessary, All other traffic is specifically denied. 	<ul style="list-style-type: none"> Examine NSC configuration standards. Examine NSC configurations. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Outbound traffic from the CDE is restricted as follows: <ul style="list-style-type: none"> To only traffic that is necessary. All other traffic is specifically denied. 	<ul style="list-style-type: none"> Examine NSC configuration standards. Examine NSC configurations. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.3	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: <ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Examine configuration settings. Examine network diagrams. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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: <ul style="list-style-type: none"> • Documented. • Kept up to date. • In use. • Known to all affected parties. 	<ul style="list-style-type: none"> • Examine documentation. • Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2 System components are configured and managed securely.						
2.2.1	Configuration standards are developed, implemented, and maintained to: <ul style="list-style-type: none"> • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment. 	<ul style="list-style-type: none"> • Examine system configuration standards. • Review industry-accepted hardening standards. • Examine configuration settings. • Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

* 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
2.2.2	<p>Vendor default accounts are managed as follows:</p> <ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Examine system configuration standards. Examine vendor documentation. Observe a system administrator logging on using vendor default accounts. Examine configuration files. Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p>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.</p> <p>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.</p>						
2.2.3	<p>Primary functions requiring different security levels are managed as follows:</p> <ul style="list-style-type: none"> Only one primary function exists on a system component, <p>OR</p> <ul style="list-style-type: none"> Primary functions with differing security levels that exist on the same system component are isolated from each other, <p>OR</p> <ul style="list-style-type: none"> Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need. 	<ul style="list-style-type: none"> Examine system configuration standards. Examine system configurations. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	<p>Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.</p>	<ul style="list-style-type: none"> Examine system configuration standards. Examine system configurations. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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: <ul style="list-style-type: none"> ▪ Business justification is documented. ▪ Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons. 	<ul style="list-style-type: none"> • Examine configuration standards. • Interview personnel. • Examine configuration settings. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	System security parameters are configured to prevent misuse.	<ul style="list-style-type: none"> • Examine system configuration standards. • Interview personnel. • Examine system configurations. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	All non-console administrative access is encrypted using strong cryptography.	<ul style="list-style-type: none"> • Examine system configuration standards. • Observe an administrator log on. • Examine system configurations. • Examine vendor documentation. • Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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: <ul style="list-style-type: none"> • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults. 	<ul style="list-style-type: none"> • Examine policies and procedures. • Review vendor documentation. • Examine wireless configuration settings. • Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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: <ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Examine key-management documentation. • Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Protect Account Data

Requirement 3: Protect Stored Account Data

Note: For SAQ C, 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: <ul style="list-style-type: none"> • Documented. • Kept up to date. • In use. • Known to all affected parties. 	<ul style="list-style-type: none"> • Examine documentation. • Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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 stored after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	<ul style="list-style-type: none"> Examine documented policies and procedures. Examine system configurations. Observe the secure data deletion processes. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes						
<i>Part of this Applicability Note was intentionally removed for this SAQ as it does not apply to merchant assessments.</i>						
Sensitive authentication data includes the data cited in Requirements 3.3.1.2 through 3.3.1.3.						
3.3.1.2	The card verification code is not stored upon completion of the authorization process.	<ul style="list-style-type: none"> Examine data sources. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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:						
<p><i>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.</i></p> <p><i>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"), mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.</i></p>						
3.3.1.3	The personal identification number (PIN) and the PIN block are not stored upon completion of the authorization process.	<ul style="list-style-type: none"> Examine data sources. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes						
PIN blocks are encrypted during the natural course of transaction processes, but even if an entity encrypts the PIN block again, it is still not allowed to be stored after the completion of the authorization process.						

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 are 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.	<ul style="list-style-type: none"> 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). 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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	Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks:					
	<ul style="list-style-type: none"> Only trusted keys and certificates are accepted. 	<ul style="list-style-type: none"> Examine documented policies and procedures. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. 	<ul style="list-style-type: none"> Interview personnel. Examine system configurations. Examine cardholder data transmissions. Examine keys and certificates. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. 		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> The encryption strength is appropriate for the encryption methodology in use. 		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes (continued)						

* 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
4.2.1 (cont.)	A self-signed certificate may also be acceptable if the certificate is issued by an internal CA within the organization, the certificate's author is confirmed, and the certificate is verified—for example, via hash or signature—and has not expired. <i>The bullet above (for confirming that certificates used to safeguard PAN during transmission over open, public networks are valid and are not expired or revoked) is a best practice until 31 March 2025, after which it will be required as part of Requirement 4.2.1 and must be fully considered during a PCI DSS assessment.</i>				
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. <ul style="list-style-type: none"> Examine system configurations. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies. <ul style="list-style-type: none"> Examine documented policies and procedures. Examine system configurations and vendor documentation. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes					
This requirement also applies if a customer, or other third-party, requests that PAN is sent to them via end-user messaging technologies. There could be occurrences where an entity receives unsolicited cardholder data via an insecure communication channel that was not intended for transmissions of sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or delete the cardholder data and implement measures to prevent the channel from being used for cardholder data.					

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
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.						
5.1.1	All security policies and operational procedures that are identified in Requirement 5 are: <ul style="list-style-type: none"> • Documented. • Kept up to date. • In use. • Known to all affected parties. 	<ul style="list-style-type: none"> • Examine documentation. • Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SAQ Completion Guidance: Selection of any of the In Place responses for Requirement 5.1.1 means that the merchant has policies and procedures in place that govern merchant activities for Requirement 5.						
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.	<ul style="list-style-type: none"> • Examine system components. • Examine the periodic evaluations. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	The deployed anti-malware solution(s): <ul style="list-style-type: none"> • Detects all known types of malware. • Removes, blocks, or contains all known types of malware. 	<ul style="list-style-type: none"> • Examine vendor documentation. • Examine system configurations. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[♦] 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
5.2.3	Any system components that are not at risk for malware are evaluated periodically to include the following: <ul style="list-style-type: none"> A documented list of all system components not at risk for malware. Identification and evaluation of evolving malware threats for those system components. Confirmation whether such system components continue to not require anti-malware protection. 	<ul style="list-style-type: none"> Examine documented policies and procedures. Interview personnel. Examine the list of system components not at risk for malware and compare against the system components without an anti-malware solution deployed. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Applicability Notes System components covered by this requirement are those for which there is no anti-malware solution deployed per Requirement 5.2.1.					
5.2.3.1	The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	<ul style="list-style-type: none"> Examine the targeted risk analysis. Examine documented results of periodic evaluations. Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Applicability Notes <i>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.</i>					
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.	<ul style="list-style-type: none"> Examine anti-malware solution(s) configurations, including any master installation. Examine system components and logs. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
5.3.2	The anti-malware solution(s): <ul style="list-style-type: none"> Performs periodic scans and active or real-time scans OR <ul style="list-style-type: none"> Performs continuous behavioral analysis of systems or processes. 	<ul style="list-style-type: none"> Examine anti-malware solution(s) configurations, including any master installation. Examine system components. Examine logs and scan results. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2.1	If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	<ul style="list-style-type: none"> Examine the targeted risk analysis. Examine documented results of periodic malware scans. Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes						
This requirement applies to entities conducting periodic malware scans to meet Requirement 5.3.2. <i>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.</i>						
5.3.3	For removable electronic media, the anti-malware solution(s): <ul style="list-style-type: none"> Performs automatic scans of when the media is inserted, connected, or logically mounted, OR <ul style="list-style-type: none"> Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted. 	<ul style="list-style-type: none"> Examine anti-malware solution(s) configurations. Examine system components with removable electronic media. Examine logs and scan results. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes						
<i>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.</i>						
5.3.4	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	<ul style="list-style-type: none"> Examine anti-malware solution(s) configurations. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
5.3.5	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.	<ul style="list-style-type: none"> Examine anti-malware configurations. Observe processes. Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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.					
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.	<ul style="list-style-type: none"> Observe implemented processes. Examine mechanisms. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Applicability Notes 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. <i>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.</i>					

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	
6.2 Bespoke and custom software are developed securely.						
<i>Note: For SAQ C, requirements at 6.2 apply to merchants with bespoke software (developed to the entity's specifications by a third party) or custom software (developed by the entity). If merchant does not have such software, mark these requirements as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.</i>						
6.2.1	<p>Bespoke and custom software are developed securely, as follows:</p> <ul style="list-style-type: none"> Based on industry standards and/or best practices for secure development. <i>Bullet intentionally left blank for this SAQ.</i> <i>Bullet intentionally left blank for this SAQ.</i> 	<ul style="list-style-type: none"> Examine documented software development procedures. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes						
This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.						
6.2.2	<p>Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:</p> <ul style="list-style-type: none"> On software security relevant to their job function and development languages. Including secure software design and secure coding techniques. Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software. 	<ul style="list-style-type: none"> Examine documented software development procedures. Examine training records. Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes (continued)						

[♦] 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	
6.2.2 (cont.)	Software development personnel remain knowledgeable about secure development practices; software security; and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.					
6.2.3.1	<p>If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:</p> <ul style="list-style-type: none"> Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices. Reviewed and approved by management prior to release. 	<ul style="list-style-type: none"> Examine documented software development procedures. Interview responsible personnel. Examine evidence of changes to bespoke and custom software. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes						
<p>Manual code reviews can be conducted by knowledgeable internal personnel or knowledgeable third-party personnel.</p> <p>An individual that has been formally granted accountability for release control and who is neither the original code author nor the code reviewer fulfills the criteria of being management.</p>						

PCI DSS Requirement	Expected Testing	Response* (Check one response for each requirement)			
		In Place	In Place with CCW	Not Applicable	Not in Place
6.2.4	Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following:				
	<ul style="list-style-type: none"> Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<ul style="list-style-type: none"> Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes					
This applies to all software developed for or by the entity for the entity’s own use. This includes both bespoke and custom software. This does not apply to third-party 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: <ul style="list-style-type: none"> • 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. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. 	<ul style="list-style-type: none"> • Examine policies and procedures. • Interview responsible personnel. • Examine documentation. • Observe processes. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes					
This requirement is not achieved by, and is in addition to, performing vulnerability scans according to 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: <ul style="list-style-type: none"> • Patches/updates for critical vulnerabilities (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • <i>Bullet intentionally left blank for this SAQ.</i> 	<ul style="list-style-type: none"> • Examine policies and procedures. • Examine system components and related software. • Compare list of security patches installed to recent vendor patch lists. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Requirement		Expected Testing	Response [†] (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
6.5.1	<p>Changes to all system components in the production environment are made according to established procedures that include:</p> <ul style="list-style-type: none"> Reason for, and description of, the change. Documentation of security impact. Documented change approval by authorized parties. Testing to verify that the change does not adversely impact system security. For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. Procedures to address failures and return to a secure state. 	<ul style="list-style-type: none"> Examine documented change control procedures. Examine recent changes to system components and trace changes to change control documentation. Examine change control documentation. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.2	<p>Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.</p>	<ul style="list-style-type: none"> Examine documentation for significant changes. Interview personnel. Observe the affected systems/networks. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes						
<i>This Applicability Note was intentionally removed as it does not apply to this SAQ.</i>						

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: <ul style="list-style-type: none"> • Job classification and function. • Least privileges necessary to perform job responsibilities. 	<ul style="list-style-type: none"> • Examine policies and procedures. • Examine user access settings, including for privileged users. • Interview responsible management personnel. • Interview personnel responsible for assigning access. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.2.3	Required privileges are approved by authorized personnel.	<ul style="list-style-type: none"> • Examine policies and procedures. • Examine user IDs and assigned privileges. • Examine documented approvals. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[♦] 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
7.2.4	<p>All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:</p> <ul style="list-style-type: none"> • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate. 	<ul style="list-style-type: none"> • Examine policies and procedures. • Interview responsible personnel. • Examine documented results of periodic reviews of user accounts. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p>This requirement applies to all user accounts and related access privileges, including those used by personnel and third parties/vendors, and accounts used to access third-party cloud services. See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts.</p> <p><i>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.</i></p>						
7.2.5	<p>All application and system accounts and related access privileges are assigned and managed as follows:</p> <ul style="list-style-type: none"> • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use. 	<ul style="list-style-type: none"> • Examine policies and procedures. • Examine privileges associated with system and application accounts. • Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p><i>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.</i></p>						

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: <ul style="list-style-type: none"> • Documented. • Kept up to date. • In use. • Known to all affected parties. 	<ul style="list-style-type: none"> • Examine documentation. • Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SAQ Completion Guidance:						
Selection of any of the <i>In Place</i> 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.	<ul style="list-style-type: none"> • Interview responsible personnel. • Examine audit logs and other evidence. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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.						

[♦] 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
<p>8.2.2 Group, shared, or generic IDs, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows:</p> <ul style="list-style-type: none"> ID 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. 	<ul style="list-style-type: none"> Examine user account lists on system components and applicable documentation. Examine authentication policies and procedures. Interview system administrators. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p>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.</p>					
<p>8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows:</p> <ul style="list-style-type: none"> Authorized with the appropriate approval. Implemented with only the privileges specified on the documented approval. 	<ul style="list-style-type: none"> Examine documented authorizations across various phases of the account lifecycle (additions, modifications, and deletions). Examine system settings. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p>This requirement applies to all user accounts, including employees, contractors, consultants, temporary workers, and third-party vendors.</p>					
<p>8.2.5 Access for terminated users is immediately revoked.</p>	<ul style="list-style-type: none"> Examine information sources for terminated users. Review current user access lists. Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
8.2.6	Inactive user accounts are removed or disabled within 90 days of inactivity.	<ul style="list-style-type: none"> Examine user accounts and last logon information. Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.7	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: <ul style="list-style-type: none"> Enabled only during the time period needed and disabled when not in use. Use is monitored for unexpected activity. 	<ul style="list-style-type: none"> Interview responsible personnel. Examine documentation for managing accounts. Examine evidence. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.2.8	If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	<ul style="list-style-type: none"> Examine system configuration settings. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes						
<p>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.</p> <p>This requirement is not meant to prevent legitimate activities from being performed while the console/PC is unattended.</p>						

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 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: <ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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. 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.					
8.3.2 Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	<ul style="list-style-type: none"> • Examine vendor documentation • Examine system configuration settings. • Examine repositories of authentication factors. • Examine data transmissions. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.3.3 User identity is verified before modifying any authentication factor.	<ul style="list-style-type: none"> • Examine procedures for modifying authentication factors. • Observe security personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Requirement	Expected Testing	Response* (Check one response for each requirement)			
		In Place	In Place with CCW	Not Applicable	Not in Place
<p>8.3.4 Invalid authentication attempts are limited by:</p> <ul style="list-style-type: none"> • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed. 	<ul style="list-style-type: none"> • Examine system configuration settings. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p>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.</p>					
<p>8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:</p> <ul style="list-style-type: none"> • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use. 	<ul style="list-style-type: none"> • Examine procedures for setting and resetting passwords/passphrases. • Observe security personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>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:</p> <ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Examine system configuration settings. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p>This requirement is not intended to apply to:</p> <ul style="list-style-type: none"> • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. • Application or system accounts, which are governed by requirements in section 8.6. <p><i>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.</i></p> <p>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.</p>					

PCI DSS Requirement		Expected Testing	Response [†] (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
8.3.7	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	<ul style="list-style-type: none"> Examine system configuration settings. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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.					
8.3.8	Authentication policies and procedures are documented and communicated to all users including: <ul style="list-style-type: none"> Guidance on selecting strong authentication factors. Guidance for how users should protect their authentication factors. Instructions not to reuse previously used passwords/passphrases. Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident. 	<ul style="list-style-type: none"> Examine procedures. Interview personnel. Review authentication policies and procedures that are distributed to users. Interview users. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Requirement	Expected Testing	Response* (Check one response for each requirement)			
		In Place	In Place with CCW	Not Applicable	Not in Place
<p>8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either:</p> <ul style="list-style-type: none"> • Passwords/passphrases are changed at least once every 90 days, <p>OR</p> <ul style="list-style-type: none"> • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. 	<ul style="list-style-type: none"> • Inspect system configuration settings. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p>This requirement does not apply to in-scope system components where MFA is used.</p> <p>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.</p> <p>This requirement does not apply to service providers' customer accounts but does apply to accounts for service provider personnel.</p>					
<p>8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.</p>	<ul style="list-style-type: none"> • Examine network and/or system configurations. • Observe administrator personnel logging into the CDE. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p>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.</p>					

PCI DSS Requirement		Expected Testing	Response [†] (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
8.4.2	<p>MFA is implemented for all non-console access into the CDE.</p>	<ul style="list-style-type: none"> Examine network and/or system configurations. Observe personnel logging in to the CDE. Examine evidence. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p>This requirement does not apply to:</p> <ul style="list-style-type: none"> Application or system accounts performing automated functions. User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. User accounts that are only authenticated with phishing-resistant authentication factors. <p>MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3. Therefore, applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access. If an individual first connects to the entity's network via remote access, and then later initiates a connection into the CDE from within the network, per this requirement the individual would authenticate using MFA twice, once when connecting via remote access to the entity's network and once when connecting from the entity's network into the CDE.</p> <p>The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function.</p> <p>MFA for access into the CDE can be implemented at the network or system/application level; it does not have to be applied at both levels. For example, if MFA is used when a user connects to the CDE network, it does not have to be used when the user logs into each system or application within the CDE.</p> <p><i>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</i></p>						

PCI DSS Requirement	Expected Testing	Response* (Check one response for each requirement)			
		In Place	In Place with CCW	Not Applicable	Not in Place
8.4.3 MFA is implemented for all remote access originating from outside the entity's network that could access or impact the CDE.	<ul style="list-style-type: none"> Examine network and/or system configurations for remote access servers and systems. Observe personnel (for example, users and administrators) and third parties connecting remotely to the network. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes The requirement for MFA for remote access originating from outside the entity's network applies to all user accounts that can access the network remotely, where that remote access leads to or could lead to access into the CDE. This includes all remote access by personnel (users and administrators), and third parties (including, but not limited to, vendors, suppliers, service providers, and customers). If remote access is to a part of the entity's network that is properly segmented from the CDE, such that remote users cannot access or impact the CDE, MFA for remote access to that part of the network is not required. However, MFA is required for any remote access to networks with access to the CDE and is recommended for all remote access to the entity's networks. The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function.					

PCI DSS Requirement	Expected Testing	Response* (Check one response for each requirement)				
		In Place	In Place with CCW	Not Applicable	Not in Place	
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.						
8.5.1	<p>MFA systems are implemented as follows:</p> <ul style="list-style-type: none"> The MFA system is not susceptible to replay attacks. MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. At least two different types of authentication factors are used. Success of all authentication factors is required before access is granted. 	<ul style="list-style-type: none"> Examine vendor system documentation. Examine system configurations for the MFA implementation. Interview responsible personnel and observe processes. Observe personnel logging into system components in the CDE. Observe personnel connecting remotely from outside the entity's network. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes						
<i>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.</i>						

PCI DSS Requirement	Expected Testing	Response* (Check one response for each requirement)			
		In Place	In Place with CCW	Not Applicable	Not in Place
8.6 Use of application and system accounts and associated authentication factors is strictly managed.					
8.6.1 If accounts used by systems or applications can be used for interactive login, they are managed as follows: <ul style="list-style-type: none"> • Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to account is granted. • Every action taken is attributable to an individual user. 	<ul style="list-style-type: none"> • Examine application and system accounts that can be used interactively. • Interview administrative personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes <i>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.</i>					

PCI DSS Requirement	Expected Testing	Response* (Check one response for each requirement)			
		In Place	In Place with CCW	Not Applicable	Not in Place
<p>8.6.2 Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.</p>	<ul style="list-style-type: none"> • Interview personnel. • Examine system development procedures. • Examine scripts, configuration/property files, and bespoke and custom source code for application and system accounts that can be used for interactive login. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p>Stored passwords/passphrases are required to be encrypted in accordance with PCI DSS Requirement 8.3.2.</p> <p><i>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.</i></p>					
<p>8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows:</p> <ul style="list-style-type: none"> • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases. 	<ul style="list-style-type: none"> • Examine policies and procedures. • Examine the targeted risk analysis. • Interview responsible personnel. • Examine system configuration settings. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p><i>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.</i></p>					

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: <ul style="list-style-type: none"> • Documented. • Kept up to date. • In use. • Known to all affected parties. 	<ul style="list-style-type: none"> • Examine documentation. • Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SAQ Completion Guidance: <i>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.</i>						
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.	<ul style="list-style-type: none"> • Observe physical entry controls. • Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes						
This requirement does not apply to locations that are publicly accessible by consumers (cardholders).						

[♦] 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
9.2.1.1	Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: <ul style="list-style-type: none"> ▪ Entry and exit points to/from sensitive areas within the CDE are monitored. ▪ Monitoring devices or mechanisms are protected from tampering or disabling. ▪ Collected data is reviewed and correlated with other entries. ▪ Collected data is stored for at least three months, unless otherwise restricted by law. 	<ul style="list-style-type: none"> • Observe locations where individual physical access to sensitive areas within the CDE occurs. • Observe the physical access control mechanisms and/or examine video cameras. • Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.2.2	Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	<ul style="list-style-type: none"> • Interview responsible personnel. • Observe locations of publicly accessible network jacks. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.						
<i>Note: For SAQ C, 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).</i>						
9.4.1	All media with cardholder data is physically secured.	<ul style="list-style-type: none"> • Examine documentation. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	<ul style="list-style-type: none"> • Examine documented procedures. • Examine logs or other documentation. • Interview responsible personnel at the storage location(s). 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4.2	All media with cardholder data is classified in accordance with the sensitivity of the data.	<ul style="list-style-type: none"> • Examine documented procedures. • Examine media logs or other documentation. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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: <ul style="list-style-type: none"> • <i>Bullet intentionally left blank for this SAQ.</i> • Media is sent by secured courier or other delivery method that can be accurately tracked. • <i>Bullet intentionally left blank for this SAQ.</i> 	<ul style="list-style-type: none"> • Examine documented procedures. • Interview personnel. • Examine records. • Examine offsite tracking logs for all media. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	<ul style="list-style-type: none"> • Examine documented procedures. • Examine offsite media tracking logs. • Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes					
9.4.4 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: <ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Examine the media destruction policy. • Observe processes. • Interview personnel. • Observe storage containers. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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.					

PCI DSS Requirement	Expected Testing	Response* (Check one response for each requirement)			
		In Place	In Place with CCW	Not Applicable	Not in Place
<p>SAQ Completion Guidance:</p> <p>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.</p> <p>If the merchant never stores any paper with account data, mark this requirement as Not Applicable and complete Appendix C: Explanation of Requirements Noted as Not Applicable.</p>					
<p>9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.</p>					
<p>9.5.1</p> <p>POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:</p> <ul style="list-style-type: none"> • Maintaining a list of POI devices. • Periodically inspecting POI devices to look for tampering or unauthorized substitution. • Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices. 	<ul style="list-style-type: none"> • Examine documented policies and procedures. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p>These requirements apply to deployed POI devices used in card-present transactions (that is, a payment card form factor such as a card that is swiped, tapped, or dipped).</p> <p>These requirements do not apply to:</p> <ul style="list-style-type: none"> • Components used only for manual PAN key entry. • Commercial off-the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution. 					
<p>9.5.1.1</p> <p>An up-to-date list of POI devices is maintained, including:</p> <ul style="list-style-type: none"> • Make and model of the device. • Location of device. • Device serial number or other methods of unique identification. 	<ul style="list-style-type: none"> • Examine the list of POI devices. • Observe POI devices and device locations. • Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Requirement		Expected Testing	Response [†] (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
9.5.1.2	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	<ul style="list-style-type: none"> Examine documented procedures. Interview responsible personnel. Observe inspection processes. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.5.1.3	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: <ul style="list-style-type: none"> Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. Procedures to ensure devices are not installed, replaced, or returned without verification. Being aware of suspicious behavior around devices. Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel. 	<ul style="list-style-type: none"> Review training materials for personnel in POI environments. Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

SAQ Completion Guidance:

Selection of any of the In Place responses for Requirements at 9.5 means that the merchant has policies and procedures in place for Requirements 9.5.1, 9.5.1.1, 9.5.1.2, and 9.5.1.3, and that they maintain a current list of devices, conduct periodic device inspections, and train employees about what to look for to detect tampered or substituted devices.

Regularly Monitor and Test Networks

Requirement 10: Log and Monitor All Access to System Components and 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	
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.						
10.1.1	All security policies and operational procedures that are identified in Requirement 10 are: <ul style="list-style-type: none"> • Documented. • Kept up to date. • In use. • Known to all affected parties. 	<ul style="list-style-type: none"> • Examine documentation. • Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.						
10.2.1.2	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	<ul style="list-style-type: none"> • Examine audit log configurations. • Examine audit log data. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.1.4	Audit logs capture all invalid logical access attempts.	<ul style="list-style-type: none"> • Examine audit log configurations. • Examine audit log data. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.1.5	Audit logs capture all changes to identification and authentication credentials including, but not limited to: <ul style="list-style-type: none"> • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access. 	<ul style="list-style-type: none"> • Examine audit log configurations. • Examine audit log data. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[♦] 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
10.2.2	Audit logs record the following details for each auditable event: <ul style="list-style-type: none"> • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol). 	<ul style="list-style-type: none"> • Interview responsible personnel. • Examine audit log configurations. • Examine audit log data. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3 Audit logs are protected from destruction and unauthorized modifications.						
10.3.1	Read access to audit logs files is limited to those with a job-related need.	<ul style="list-style-type: none"> • Interview system administrators • Examine system configurations and privileges. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.2	Audit log files are protected to prevent modifications by individuals.	<ul style="list-style-type: none"> • Examine system configurations and privileges. • Interview system administrators. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.4	File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.	<ul style="list-style-type: none"> • Examine system settings. • Examine monitored files. • Examine results from monitoring activities. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.4.1	The following audit logs are reviewed at least once daily: <ul style="list-style-type: none"> • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers). 	<ul style="list-style-type: none"> • Examine security policies and procedures. • Observe processes. • Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
10.4.1.1	Automated mechanisms are used to perform audit log reviews.	<ul style="list-style-type: none"> Examine log review mechanisms. Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Applicability Notes					
	<i>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.</i>					
10.4.2	Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.	<ul style="list-style-type: none"> Examine security policies and procedures. Examine documented results of log reviews. Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Applicability Notes					
	This requirement is applicable to all other in-scope system components not included in Requirement 10.4.1.					
10.4.2.1	The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	<ul style="list-style-type: none"> Examine the targeted risk analysis. Examine documented results of periodic log reviews. Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Applicability Notes					
	<i>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.</i>					
10.4.3	Exceptions and anomalies identified during the review process are addressed.	<ul style="list-style-type: none"> Examine security policies and procedures. Observe processes. Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Requirement	Expected Testing	Response* (Check one response for each requirement)				
		In Place	In Place with CCW	Not Applicable	Not in Place	
10.5 Audit log history is retained and available for analysis.						
10.5.1	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	<ul style="list-style-type: none"> Examine documented audit log retention policies and procedures. Examine configurations of audit log history. Examine audit logs. Interview personnel. Observe processes. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6 Time-synchronization mechanisms support consistent time settings across all systems.						
10.6.1	System clocks and time are synchronized using time-synchronization technology.	<ul style="list-style-type: none"> Examine system configuration settings. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Applicability Notes Keeping time-synchronization technology current includes managing vulnerabilities and patching the technology according to PCI DSS Requirements 6.3.1 and 6.3.3.					
10.6.2	Systems are configured to the correct and consistent time as follows: <ul style="list-style-type: none"> One or more designated time servers are in use. Only the designated central time server(s) receives time from external sources. Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). The designated time server(s) accept time updates only from specific industry-accepted external sources. Where there is more than one designated time server, the time servers peer with one another to keep accurate time. Internal systems receive time information only from designated central time server(s). 	<ul style="list-style-type: none"> Examine system configuration settings for acquiring, distributing, and storing the correct time. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
10.6.3	Time synchronization settings and data are protected as follows: <ul style="list-style-type: none"> • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed. 	<ul style="list-style-type: none"> • Examine system configurations and time-synchronization settings and logs. • Observe processes. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Requirement 11: Test Security of Systems and Networks Regularly

PCI DSS Requirement	Expected Testing	Response [♦] (Check one response for each requirement)				
		In Place	In Place with CCW	Not Applicable	Not in Place	
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.						
11.2.1	<p>Authorized and unauthorized wireless access points are managed as follows:</p> <ul style="list-style-type: none"> The presence of wireless (Wi-Fi) access points is tested for. All authorized and unauthorized wireless access points are detected and identified. Testing, detection, and identification occurs at least once every three months. If automated monitoring is used, personnel are notified via generated alerts. <p>Applicability Notes</p> <p>The requirement applies even when a policy exists that prohibits the use of wireless technology. Methods used to meet this requirement must be sufficient to detect and identify both authorized and unauthorized devices, including unauthorized devices attached to devices that themselves are authorized.</p>	<ul style="list-style-type: none"> Examine policies and procedures. Examine the methodology(ies) in use and the resulting documentation. Interview personnel. Examine wireless assessment results. Examine configuration settings. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.2	<p>An inventory of authorized wireless access points is maintained, including a documented business justification.</p>	<ul style="list-style-type: none"> Examine documentation. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[♦] 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
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.					
11.3.1 Internal vulnerability scans are performed as follows: <ul style="list-style-type: none"> • At least once every three months. • Vulnerabilities that are either high-risk or critical (according to the entity’s vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high-risk and critical vulnerabilities as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists. 	<ul style="list-style-type: none"> • Examine internal scan report results. • Examine scan tool configurations. • Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes It is not required to use a QSA or ASV to conduct internal vulnerability scans. Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned (for example, a network administrator should not be responsible for scanning the network), or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.					
11.3.1.3 Internal vulnerability scans are performed after any significant change as follows: <ul style="list-style-type: none"> • Vulnerabilities that are either high-risk or critical (according to the entity’s vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV). 	<ul style="list-style-type: none"> • Examine change control documentation. • Interview personnel. • Examine internal scan and rescan report as applicable. • Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes <i>Applicability Note intentionally left blank for this SAQ.</i>					

PCI DSS Requirement	Expected Testing	Response* (Check one response for each requirement)			
		In Place	In Place with CCW	Not Applicable	Not in Place
<p>11.3.2 External vulnerability scans are performed as follows:</p> <ul style="list-style-type: none"> • At least once every three months. • By PCI SSC Approved Scanning Vendor (ASV) • Vulnerabilities are resolved and <i>ASV Program Guide</i> requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the <i>ASV Program Guide</i> requirements for a passing scan. 	<ul style="list-style-type: none"> • Examine ASV scan reports. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>Applicability Notes</p> <p>For the initial PCI DSS assessment against this requirement, it is not required that four passing scans be completed within 12 months if the assessor verifies: 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring scanning at least once every three months, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s).</p> <p>However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred.</p> <p>ASV scanning tools can scan a vast array of network types and topologies. Any specifics about the target environment (for example, load balancers, third-party providers, ISPs, specific configurations, protocols in use, scan interference) should be worked out between the ASV and scan customer.</p> <p>Refer to the <i>ASV Program Guide</i> published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.</p>					
<p>11.3.2.1 External vulnerability scans are performed after any significant change as follows:</p> <ul style="list-style-type: none"> • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV). 	<ul style="list-style-type: none"> • Examine change control documentation. • Interview personnel. • Examine external scan, and as applicable rescan reports. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

PCI DSS Requirement	Expected Testing	Response* (Check one response for each requirement)			
		In Place	In Place with CCW	Not Applicable	Not in Place
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.					
11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: <ul style="list-style-type: none"> • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use. • <i>Bullet intentionally left blank for this SAQ.</i> • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV). 	<ul style="list-style-type: none"> • Examine segmentation controls. • Review penetration-testing methodology. • Examine the results from the most recent penetration test. • Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.5 Network intrusions and unexpected file changes are detected and responded to.					
11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: <ul style="list-style-type: none"> • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly. 	<ul style="list-style-type: none"> • Examine system settings for the change-detection mechanism. • Examine monitored files. • Examine results from monitoring activities. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes (continued)					

PCI DSS Requirement		Expected Testing	Response [†] (Check one response for each requirement)			
			In Place	In Place with CCW	Not Applicable	Not in Place
11.5.2 (cont.)	For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).					

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: <ul style="list-style-type: none"> Established. Published. Maintained. Disseminated to all relevant personnel, as well as to relevant vendors and business partners. 	<ul style="list-style-type: none"> Examine the information security policy. Interview personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.1.2	The information security policy is: <ul style="list-style-type: none"> Reviewed at least once every 12 months. Updated as needed to reflect changes to business objectives or risks to the environment 	<ul style="list-style-type: none"> Examine the information security policy. Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.

For example, such a policy could be a simple document that covers how to protect the store and payment devices in accordance with the solution provider’s guidance/instruction manual, and who to call in an emergency.

[♦] 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
12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	<ul style="list-style-type: none"> Examine the information security policy. Interview responsible personnel. Examine documented evidence. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SAQ Completion Guidance: <i>Selection of any of the In Place responses for Requirement 12.1.3 means that the merchant's security policy defines basic security responsibilities for all personnel, consistent with the size and complexity of the merchant's operations. For example, security responsibilities could be defined according to basic responsibilities by employee levels, such as the responsibilities expected of a manager/owner and those expected of clerks.</i>					
12.2 Acceptable use policies for end-user technologies are defined and implemented.					
12.2.1 Acceptable use policies for end-user technologies are documented and implemented, including: <ul style="list-style-type: none"> Explicit approval by authorized parties. Acceptable uses of the technology. List of products approved by the company for employee use, including hardware and software. 	<ul style="list-style-type: none"> Examine acceptable use policies. Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes Examples of end-user technologies for which acceptable use policies are expected include, but are not limited to, remote access and wireless technologies, laptops, tablets, mobile phones, and removable electronic media, e-mail usage, and Internet usage.					

PCI DSS Requirement	Expected Testing	Response* (Check one response for each requirement)				
		In Place	In Place with CCW	Not Applicable	Not in Place	
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.						
12.3.1	<p>For each PCI DSS requirement that specifies completion of a targeted risk analysis, the analysis is documented and includes:</p> <ul style="list-style-type: none"> • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for how the frequency or processes defined by the entity to meet the requirement minimize the likelihood and/or impact of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review. 	<ul style="list-style-type: none"> • Examine documented policies and procedures. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes						
<i>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.</i>						

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.	<ul style="list-style-type: none"> Examine the security awareness program. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SAQ Completion Guidance: <i>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.</i>						
12.6.3.1	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the cardholder data and/or sensitive authentication data, including but not limited to: <ul style="list-style-type: none"> Phishing and related attacks. Social engineering. 	<ul style="list-style-type: none"> Examine security awareness training content. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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. <i>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.</i>						

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.	<ul style="list-style-type: none"> Examine policies and procedures. Examine list of TPSPs. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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: <ul style="list-style-type: none"> 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 TPSPs 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 the TPSP could impact the security of the entity's cardholder data and/or sensitive authentication data. 	<ul style="list-style-type: none"> Examine policies and procedures. Examine written agreements with TPSPs. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicability Notes The exact wording of an agreement will depend the details of the service being provided, and the responsibilities assigned to each party. The agreement does not have to include the exact wording provided in this requirement. The TPSP's written acknowledgment is a confirmation that states the TPSP is responsible for the security of the account data it may store, process, or transmit on behalf of the customer or to the extent the TPSP may impact the security of a customer's cardholder data and/or sensitive authentication data. Evidence that a TPSP is meeting PCI DSS requirements is not the same as a written acknowledgment specified in this requirement. For example, a PCI DSS Attestation of Compliance (AOC), a declaration on a company's website, a policy statement, a responsibility matrix, or other evidence not included in a written agreement is not a written acknowledgment.					

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.	<ul style="list-style-type: none"> Examine policies and procedures. Examine evidence. Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.4	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	<ul style="list-style-type: none"> Examine policies and procedures. Examine documentation. Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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.	<ul style="list-style-type: none"> Examine policies and procedures. Examine documentation. Interview responsible personnel. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

SAQ Completion Guidance:

Selection of any of the In Place responses for requirements at 12.8.1 through 12.8.5 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.

PCI DSS Requirement	Expected Testing	Response* (Check one response for each requirement)				
		In Place	In Place with CCW	Not Applicable	Not in Place	
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.						
12.10.1	<p>An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to:</p> <ul style="list-style-type: none"> • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands. 	<ul style="list-style-type: none"> • Examine the incident response plan. • Interview personnel. • Examine documentation from previously reported incidents. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>SAQ Completion Guidance:</p> <p><i>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.</i></p>						
12.10.3	<p>Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.</p>	<ul style="list-style-type: none"> • Interview responsible personnel. • Examine documentation. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

PCI DSS Requirement	Expected Testing	Response [♦] (Check one response for each requirement)				
		In Place	In Place with CCW	Not Applicable	Not in Place	
A2.1 POI terminals using SSL and/or early TLS are not susceptible to known SSL/TLS exploits.						
A2.1.1	<p>Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols.</p> <p>Applicability Notes</p> <p>This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requirement is not intended for service providers who serve as the termination or connection point to those POS POI terminals. Requirements A2.1.2 and A2.1.3 apply to POS POI service providers.</p> <p>The allowance for POS POI terminals that are not currently susceptible to exploits is based on currently known risks. If new exploits are introduced to which POS POI terminals are susceptible, the POS POI terminals will need to be updated immediately.</p>	<ul style="list-style-type: none"> Examine documentation (for example, vendor documentation, system/network configuration details) that verifies the devices are not susceptible to any known exploits for SSL/early TLS. 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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 D: Explanation of Requirements Noted as Not Tested

This Appendix is not used for SAQ C merchant assessments.

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ C (Section 2), dated (Self-assessment completion date YYYY-MM-DD).

Based on the results documented in the SAQ C 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:

<input type="checkbox"/>	<p>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 (<i>Merchant Company Name</i>) has demonstrated compliance with all PCI DSS requirements included in this SAQ.</p>								
<input type="checkbox"/>	<p>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 (<i>Merchant Company Name</i>) has not demonstrated compliance with the PCI DSS requirements included in this SAQ.</p> <p>Target Date for Compliance: YYYY-MM-DD</p> <p>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 <i>before completing Part 4</i>.</p>								
<input type="checkbox"/>	<p>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 (<i>Merchant Company Name</i>) has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not in Place due to a legal restriction.</p> <p>This option requires additional review from the entity to which this AOC will be submitted. <i>If selected, complete the following:</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								

Part 3a. Merchant Acknowledgement

Signatory(s) confirms:

(Select all that apply)

<input type="checkbox"/>	PCI DSS Self-Assessment Questionnaire C, Version 4.0.1, was completed according to the instructions therein.
<input type="checkbox"/>	All information within the above-referenced SAQ and in this attestation fairly represents the results of the merchant's assessment in all material respects.
<input type="checkbox"/>	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:	<input type="checkbox"/> QSA performed testing procedures.
	<input type="checkbox"/> 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:	<input type="checkbox"/> ISA(s) performed testing procedures.
	<input type="checkbox"/> 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections.	<input type="checkbox"/>	<input type="checkbox"/>	

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

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance-accepting organization to ensure that this form is acceptable in its program. For more information about PCI SSC and our stakeholder community please visit: <https://www.pcisecuritystandards.org/about-us/>.