Payment Card Industry

Data Security Standard

Self-Assessment Questionnaire D for Merchants and Attestation of Compliance

For use with PCI DSS Version 4.0

Revision 1

Publication Date: December 2022

Document Changes

Date	PCI DSS Version	SAQ Revision	Description
October 2008	1.2		To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 2010	2.0		To align content with new PCI DSS v2.0 requirements and testing procedures.
February 2014	3.0		To align content with PCI DSS v3.0 requirements and testing procedures and incorporate additional response options.
April 2015	3.1		Updated to align with PCI DSS v3.1. For details of PCI DSS changes, see PCI DSS - Summary of Changes from PCI DSS Version 3.0 to 3.1.
July 2015	3.1	1.1	Updated to remove references to "best practices" prior to June 30, 2015, and remove the PCI DSS v2 reporting option for Requirement 11.3.
April 2016	3.2	1.0	Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see PCI DSS - Summary of Changes from PCI DSS Version 3.1 to 3.2.
January 2017	3.2	1.1	Updated version numbering to align with other SAQs
June 2018	3.2.1	1.0	Updated to align with PCI DSS v3.2.1. For details of PCI DSS changes, see PCI DSS - Summary of Changes from PCI DSS Version 3.2 to 3.2.1.
April 2022	4.0		Updated to align with PCI DSS v4.0. For details of PCI DSS changes, see PCI DSS - Summary of Changes from PCI DSS Version 3.2.1 to 4.0. Rearranged, retitled, and expanded information in the "Completing the Self-Assessment Questionnaire" section (previously titled "Before You Begin"). Aligned content in Sections 1 and 3 of Attestation of Compliance (AOC) with PCI DSS v4.0 Report on Compliance AOC. Added appendices to support new reporting responses.
December 2022	4.0	1	Removed "In Place with Remediation" as a reporting option from Requirement Responses table, Attestation of Compliance (AOC) Part 2g, SAQ Section 2 Response column, and AOC Section 3. Also removed former Appendix C. Added "In Place with CCW" to AOC Section 3. Added guidance for responding to future-dated requirements. Added minor clarifications and addressed typographical errors.

Contents

Completing the Self-Assessment Questionnaire

Merchant Eligibility Criteria for Self-Assessment Questionnaire D

Self-Assessment Questionnaire (SAQ) D for Merchants applies to merchants that are eligible to complete a self-assessment questionnaire but do not meet the criteria for any other SAQ type. Examples of merchant environments to which SAQ D may apply include but are not limited to:

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

This SAQ is not applicable to service providers.

Defining Account Data, Cardholder Data, and Sensitive Authentication Data

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

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

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

PCI DSS Self-Assessment Completion Steps

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

Expected Testing

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

The intent behind each testing method is described as follows:

- Examine: The merchant critically evaluates data evidence. Common examples include documents (electronic or physical), screenshots, configuration files, audit logs, and data files.
- Observe: The merchant watches an action or views something in the environment. Examples of observation subjects include personnel performing a task or process, system components performing a function or responding to input, environmental conditions, and physical controls.
- Interview: The merchant converses with individual personnel. Interview objectives may include confirmation of whether an activity is performed, descriptions of how an activity is performed, and whether personnel have particular knowledge or understanding.

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

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

Requirement Responses

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

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

Response	When to use this response:
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated.
In Place with CCW (Compensating Controls Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Controls Worksheet (CCW) in Appendix B of this SAQ. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in PCI DSS in Appendices B and C.
Not Applicable	The requirement does not apply to the merchant's environment. (See "Guidance for Not Applicable Requirements" below for examples.) All responses in this column require a supporting explanation in Appendix C of this SAQ.
Not Tested	The requirement was not included for consideration in the assessment and was not tested in any way. (See "Understanding the Difference between Not Applicable and Not Tested" below for examples of when this option should be used.) All responses in this column require a supporting explanation in Appendix D of this SAQ.
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before the merchant can confirm they are in place. Responses in this column may require the completion of Part 4, if requested by the entity to which this SAQ will be submitted. This response is also used if a requirement cannot be met due to a legal restriction. (See "Legal Exception" below for more guidance).

Guidance for Not Applicable Requirements

While many merchants completing SAQ D will need to validate compliance with every PCI DSS requirement, some entities with very specific business models may find that some requirements do not apply. For example, entities that do not use wireless technology in any capacity are not expected to comply with the PCI DSS requirements that are specific to managing wireless technology. Similarly, entities that do not store any account data electronically at any time are not expected to comply with the PCI DSS requirements related to secure storage of account data (for example, Requirement 3.5.1). Another example is requirements specific to application development and secure coding (for example, Requirements 6.2.1 through 6.2.4), which only apply to an entity with bespoke software (developed for the entity by a third party per the entity's specifications) or custom software (developed by the entity for its own use).

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

Understanding the Difference between Not Applicable and Not Tested

Requirements that are deemed to be not applicable to an environment must be verified as such. Using the wireless example above, for a merchant to select "Not Applicable" for Requirements 1.3.3, 2.3.1, 2.3.2, and 4.2.1.2, the merchant first needs to confirm that there are no wireless technologies used in its cardholder data environment (CDE) or that connect to their CDE. Once this has been confirmed, the merchant may select "Not Applicable" for those specific requirements.

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

- A merchant is asked by their acquirer to validate a subset of requirements-for example, using the PCI DSS Prioritized Approach to validate only certain milestones.
- A merchant is confirming a new security control that impacts only a subset of requirements-for example, implementation of a new encryption methodology that only requires assessment of PCI DSS Requirements 2, 3, and 4.

In these scenarios, the merchant's assessment only includes certain PCI DSS requirements even though other requirements might also apply to its environment.

If any requirements are completely excluded from the merchant's self-assessment, select Not Tested for that specific requirement, and complete Appendix D: Explanation of Requirements Not Tested for each "Not Tested" entry. An assessment with any Not Tested responses is a "Partial" PCI DSS assessment and will be noted as such by the merchant in the Attestation of Compliance in Section 3, Part 3 of this SAQ.

Guidance for Responding to Future Dated Requirements

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

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

Legal Exception

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

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

Contractual obligations or legal advice are not legal restrictions.

Use of the Customized Approach

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

Use of the Customized Approach is not supported in SAQs.

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

Additional PCI SSC Resources

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

Resource	Includes:
PCI Data Security Standard Requirements and Testing Procedures (PCI DSS)	• Guidance on Scoping • Guidance on the intent of all PCI DSS Requirements • Details of testing procedures • Guidance on Compensating Controls • Appendix G: Glossary of Terms, Abbreviations, and Acronyms
SAQ Instructions and Guidelines	• Information about all SAQs and their eligibility criteria • How to determine which SAQ is right for your organization
Frequently Asked Questions (FAQs)	• Guidance and information about SAQs.
Online PCI DSS Glossary	• PCI DSS Terms, Abbreviations, and Acronyms

Information Supplements and Guidelines	• Guidance on a variety of PCI DSS topics including
	  • Understanding PCI DSS Scoping and Network Segmentation
	  • Third-Party Security Assurance
	  • Multi-Factor Authentication Guidance
	  • Best Practices for Maintaining PCI DSS Compliance

Getting Started with PCI	• Resources for smaller merchants including:
	  • Guide to Safe Payments
	  • Common Payment Systems
	  • Questions to Ask Your Vendors
	  • Glossary of Payment and Information Security Terms
	  • PCI Firewall Basics

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

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

Section 1: Assessment Information

Instructions for Submission

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

Part 1. Contact Information	
Part 1a. Assessed Merchant	
Company Name:	Moore Response
DBA (doing business as):	
Company mailing address:	100 Jamison Court Hagerstown Maryland 21740 USA
Company main website:	
Company contact name:	Scott Manley
Company contact title:	Security and Compliance Manager
Contact phone number:	888-966-7935
Contact e-mail address:	MooreITsecurity@wearemoore.com
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.

- [x] Mail order/telephone order (MOTO)
- [ ] E-Commerce
- [ ] Card-present

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

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

Part 2b. Description of Role with Payment Cards

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

Channel	How Business Stores, Processes, and/or Transmits Account Data
Mail/telephone ,	Response Management Group DC (RMG DC) performs Mail Order and Call Center phone processing of check and credit card payments /donations, as well as receives secured electronic files via secure methods from third parties (RMG's clients and/or its clients' selected vendors). Phone calls are recorded but paused by the call center operator when cardholder data information is exchanged, PAN is never recorded RMG transmits these transactions (HTTPS, TLS v1.2 AES 256-bit) taken over the phone and entered into a workstation with a secure browser connection. The cardholder data (PAN, Expiration Date, and Name) for the scanned images is stored unencrypted in Opex proprietary databases (CCW in use) and flat files (ltemAge) stored encrypted on servers (RMGITST01 and RMGITST02) encrypted using client supplied PGP RSA 2048-bit public encryption key. These ltemAge flat files are additionally secured by storing them on drives (RMGITST01 and RMGITST02) that are encrypted using Bitlocker AES 256-bit. RMG has a compensating control implemented (Requirement 3.4.b) as encryption cannot be used because it would not allow the Opex scanning machines to function at necessary speeds. Backup tapes are encrypted with PGP/AES 256-bit encryption because the files backed up are initially encrypted with RMG's clients' public. SAD is not requested by RMG for any mail or call center donations. If received, it is immediately destroyed by crosscut shredding and removing the SAD from the form (tearing it off to separate it from the rest of the card data). The forms are placed in secure shredding

	bins which are locked. Iron Mountain is who crosscut shreds all paper forms. For Settlement, truncated PAN is received in a text delimited file as part of the settlement process and is deleted after the settlement totals balance. The settlement files exist for a very short time (usually only hour(s)) and then are deleted using a secure deletion method.

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.	Firewalls Routers Web Servers Databases Log servers IDS WAP FIM Scanners VLAN Workstations Processor connections Encryption mechanisms and key storage
Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)*	☒ Yes ☐ No

Part 2. Executive Summary *(continued)*

Part 2d. In-Scope Locations/Facilities

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

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

Part 2e. PCI SSC Validated Products and Solutions

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

☐ Yes ☐ No

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

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

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

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers

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

If Yes:

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

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

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (SAQ Section 2 and related appendices)

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

PCI DSS Requirement *	Requirement Responses More than one response may be selected for a given requirement. Indicate all responses that apply.				
	In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
Requirement 1:	☑	☐	☐	☐	☐
Requirement 2:	☑	☐	☐	☐	☐
Requirement 3:	☑	☐	☑	☐	☐
Requirement 4:	☑	☐	☑	☐	☐
Requirement 5:	☑	☐	☑	☐	☐
Requirement 6:	☑	☐	☑	☐	☐
Requirement 7:	☑	☐	☑	☐	☐
Requirement 8:	☑	☐	☑	☐	☐
Requirement 9:	☑	☐	☑	☐	☐
Requirement 10:	☑	☐	☑	☐	☐
Requirement 11:	☑	☐	☑	☐	☐
Requirement 12:	☑	☐	☑	☐	☐
Appendix A2:	☐	☐	☑	☐	☐

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

Section 2: Self-Assessment Questionnaire D

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

Self-assessment completion date: 03/04/2024

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 Tested	Not in Place
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.							
1.1.1	All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☑	☐	☐	☐	☐
1.1.2	Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood	• Examine documentation. • Interview responsible personnel.	☑	☐	☐	☐	☐
1.2 Network security controls (NSCs) are configured and maintained.							
		• Examine configurations standards.					

1.2.1	Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.	• Examine configuration settings.	☑	☐	☐	☐	☐
1.2.2	All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.	• Examine documented procedures. • Examine network configurations. • Examine change control records. • Interview responsible personnel.	☑	☐	☐	☐	☐
	Applicability Notes Changes to network connections include the addition, removal, or modification of a connection. Changes to NSC configurations include those related to the component itself as well as those affecting how it performs its security function.						
1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	• Examine network diagrams. • Examine network configurations. • Interview responsible personnel	☑	☐	☐	☐	☐
	Applicability Notes A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement.						
1.2.4	An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment.	• Examine data flow diagrams. • Observe network configurations. • Examine documentation. • Interview responsible personnel.	☑	☐	☐	☐	☐

	Applicability Notes A data-flow diagram(s) or other technical or topological solution that identifies flows of account data across systems and networks can be used to meet this requirement.						
1.2.5	All services, protocols and ports allowed are identified, approved, and have a defined business need.	• Examine documentation. • Examine configuration settings	☑	☐	☐	☐	☐
1.2.6	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	• Examine documentation. • Examine configuration settings.	☑	☐	☐	☐	☐
1.2.7	Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	• Examine documented procedures. • Examine documentation from reviews performed. • Examine configuration settings.	☑	☐	☐	☐	☐
1.2.8	Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations	• Examine NSC configuration files.	☑	☐	☐	☐	☐
	Applicability Notes						

	Any file or setting used to configure or synchronize NSCs is considered to be a "configuration file." This includes files, automated and system-based controls, scripts, settings, infrastructure as code, or other parameters that are backed up, archived, or stored remotely.						
1.3 Network access to and from the cardholder data environment is restricted							
1.3.1	Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary, • All other traffic is specifically denied.	• Examine NSC configuration standards. • Examine NSC configurations.	☑	☐	☐	☐	☐
1.3.2	Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	• Examine NSC configuration standards. • Examine NSC configurations.	☑	☐	☐	☐	☐
1.3.3	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.	• Examine configuration settings. • Examine network diagrams.	☑	☐	☐	☐	☐
1.4 Network connections between trusted and untrusted networks are controlled.							
1.4.1	NSCs are implemented between trusted and untrusted networks.	• Examine NSC configuration standards.	☑	☐	☐	☐	☐

		• Examine current network diagrams. • Examine network configurations.					
1.4.2	Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied. Applicability Notes The intent of this requirement is to address communication sessions between trusted and untrusted networks, rather than the specifics of protocols. This requirement does not limit the use of UDP or other connectionless network protocols if state is maintained by the NSC.	• Examine NSC documentation. • Examine NSC configurations.	☑	☐	☐	☐	☐
1.4.3	Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	• Examine NSC documentation. • Examine NSC configurations.	☑	☐	☐	☐	☐
1.4.4	System components that store cardholder data are not directly accessible from untrusted networks. Applicability Notes	• Examine the data-flow diagram and network diagram. • Examine NSC configurations.	☑	☐	☐	☐	☐

	This requirement is not intended to apply to storage of account data in volatile memory but does apply where memory is being treated as persistent storage (for example, RAM disk). Account data can only be stored in volatile memory during the time necessary to support the associated business process (for example, until completion of the related payment card transaction).						
1.4.5	The disclosure of internal IP addresses and routing information is limited to only authorized parties.	• Examine NSC configurations. • Examine documentation. • Interview responsible personnel.	☑	☐	☐	☐	☐
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.							
1.5.1	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows. • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	• Examine policies and configuration standards. • Examine device configuration settings.	☑	☐	☐	☐	☐
	Applicability Notes						
	These security controls may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If these security controls need to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which these security controls are not						

	active. This requirement applies to employee-owned and company-owned computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit.					

** 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 Tested	Not in Place
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.							
2.1.1	All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☑	☐	☐	☐	☐
2.1.2	Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☑	☐	☐	☐	☐
2.2 System components are configured and managed securely							
2.2.1	Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities.	• Examine system configuration standards. • Review industry-accepted hardening standards. • Examine configuration settings.	☑	☐	☐	☐	☐

	• 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.	• Interview personnel.					
2.2.2	Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.	• Examine system configuration standards. • Examine vendor documentation. • Observe a system administrator logging on using vendor default accounts. • Examine configuration files. • Interview personnel.	☑	☐	☐	☐	☐
	Applicability Notes This applies to ALL vendor default accounts and passwords, including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Management Protocol (SNMP) defaults. This requirement also applies where a system component is not installed within an entity's environment, for example, software and applications that are part of the CDE and are accessed via a cloud subscription service.						
2.2.3	Primary functions requiring different security levels are managed as follows:	• Examine system configuration standards. • Examine system configurations.	☑	☐	☐	☐	☐

	• Only one primary function exists on a system component, OR • Primary functions with differing security levels that exist on the same system component are isolated from each other, OR • 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.						
2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	• Examine system configuration standards. • Examine system configurations.	☑	☐	☐	☐	☐
2.2.5	If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	• Examine configuration standards. • Interview personnel. • Examine configuration settings.	☑	☐	☐	☐	☐
2.2.6	System security parameters are configured to prevent misuse.	• Examine system configuration standards. • Interview personnel. • Examine system configurations.	☑	☐	☐	☐	☐

2.2.7	All non-console administrative access is encrypted using strong cryptography. Applicability Notes This includes administrative access via browser-based interfaces and application programming interfaces (APIs).	• Examine system configuration standards. • Observe an administrator log on. • Examine system configurations. • Examine vendor documentation. • Interview personnel.	☑	☐	☐	☐	☐
2.3 Wireless environments are configured and managed securely							
2.3.1	For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults. 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.	• Examine policies and procedures. • Review vendor documentation. • Examine wireless configuration settings. • Interview personnel.	☑	☐	☐	☐	☐
2.3.2	For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows:	• Examine key-management documentation. • Interview personnel.	☑	☐	☐	☐	☐

	• 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						

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

Protect Account Data

Requirement 3: Protect Stored Account Data

PCI DSS Requirement		Expected Testing	Response: (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
3.1 Processes and mechanisms for protecting stored account data are defined and understood							
3.1.1	All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties	• Examine documentation. • Interview personnel.	☑	☐	☐	☐	☐
3.1.2	Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☑	☐	☐	☐	☐
3.2 Storage of account data is kept to a minimum.							
3.2.1	Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization.	• Examine the data retention and disposal policies, procedures, and processes. • Interview personnel. • Examine files and system records on system components where account data is stored.	☑	☐	☐	☐	☐

	This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	• Observe the mechanisms used to render account data unrecoverable.					
	Applicability Notes Where account data is stored by a TPSP (for example, in a cloud environment), entities are responsible for working with their service providers to understand how the TPSP meets this requirement for the entity. Considerations include ensuring that all geographic instances of a data element are securely deleted. The bullet above (for coverage of SAD stored prior to completion of authorization) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.						
3.3 Sensitive authentication data (SAD) is not stored after authorization							
3.3.1	SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	• Examine documented policies and procedures. • Examine system configurations. • Observe the secure data deletion processes.	☑	☐	☐	☐	☐

	Applicability Notes Part of this Applicability Note was intentionally removed for this SAQ as it does not apply to merchant assessments. Sensitive authentication data includes the data cited in Requirements 3.3.1.1 through 3.3.1.3.						
3.3.1.1	The full contents of any track are not retained upon completion of the authorization process.	• Examine data sources.	☑	☐	☐	☐	☐
	Applicability Notes In the normal course of business, the following data elements from the track may need to be retained: • Cardholder name. • Primary account number (PAN). • Expiration date. • Service code. To minimize risk, store securely only these data elements as needed for business.						
3.3.1.2	The card verification code is not retained upon completion of the authorization process.	• Examine data sources.	☑	☐	☐	☐	☐
	Applicability Notes The card verification code is the three- or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions.						
3.3.1.3	The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.	• Examine data sources.	☑	☐	☐	☐	☐

	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.						
3.3.2	SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography. Applicability Notes Whether SAD is permitted to be stored prior to authorization is determined by the organizations that manage compliance programs (for example, payment brands and acquirers). Contact the organizations of interest for any additional criteria. This requirement applies to all storage of SAD, even if no PAN is present in the environment. Refer to Requirement 3.2.1 for an additional requirement that applies if SAD is stored prior to completion of authorization. *Part of this Applicability Note was intentionally removed for this SAQ as it does not apply to merchant assessments.* This requirement does not replace how PIN blocks are required to be managed, nor does it mean that a properly encrypted PIN block needs to be encrypted again. 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.	• Examine data stores and system configurations. • Examine vendor documentation.	☐	☐	☑	☐	☐
3.4 Access to displays of full PAN and ability to copy PAN is restricted.							
3.4.1	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	• Examine documented policies and procedures. • Examine system configurations. • Examine the documented list of roles that need access to more than the BIN and last four digits of the PAN (includes full PAN). • Examine displays of PAN (for example, on screen, on paper receipts).	☑	☐	☐	☐	☐

	Applicability Notes This requirement does not supersede stricter requirements in place for displays of cardholder data-for example, legal or payment brand requirements for point-of-sale (POS) receipts. This requirement relates to protection of PAN where it is displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.5.1 for protection of PAN when stored, processed, or transmitted						
3.4.2	When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need. Applicability Notes Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. 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.	• Examine documented policies and procedures and documented evidence for technical controls. • Examine configurations for remote-access technologies. • Observe processes. • Interview personnel.	☐	☐	☑	☐	☐
3.5 Primary account number (PAN) is secured wherever it is stored.							
3.5.1	PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). • If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN	• Examine documentation about the system used to render PAN unreadable. • Examine data repositories. • Examine audit logs, including payment application logs. • Examine controls to verify that the hashed and truncated PANs cannot be correlated to reconstruct the original PAN.	☑	☐	☐	☐	☐

	• Index tokens. • Strong cryptography with associated keymanagement processes and procedures.						
	Applicability Notes It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs) must all be protected. This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN						
3.5.1.1	Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1), are keyed cryptographic hashes of the entire PAN, with associated keymanagement processes and procedures in accordance with Requirements 3.6 and 3.7.	• Examine documentation about the hashing method used. • Examine documentation about the keymanagement procedures and processes. • Examine data repositories. • Examine audit logs, including payment application logs.	☐	☐	☑	☐	☐
	Applicability Notes This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs) must all be protected. This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN. This requirement is considered a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
3.5.1.2	If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is	• Observe encryption processes.	☐	☐	☑	☐	☐

	used to render PAN unreadable, it is implemented only as follows: • On removable electronic media. OR • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.	• Examine configurations and/or vendor documentation. • Observe encryption processes.					
	Applicability Notes						
	While disk encryption may still be present on these types of devices, it cannot be the only mechanism used to protect PAN stored on those systems. Any stored PAN must also be rendered unreadable per Requirement 3.5.1-for example, through truncation or a datalevel encryption mechanism. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is appropriate only for removable electronic media storage devices. Media that is part of a data center architecture (for example, hot-swappable drives, bulk tape-backups) is considered non-removable electronic media to which Requirement 3.5.1 applies. Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements. 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.						
3.5.1.3	If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.	• Examine system configurations. • Observe the authentication process. • Examine files containing authentication factors. • Interview personnel.	☐	☐	☑	☐	☐

	Applicability Notes Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.						
3.6 Cryptographic keys used to protect stored account data are secured.							
3.6.1	Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from dataencrypting keys. • Keys are stored securely in the fewest possible locations and forms	• Examine documented key-management policies and procedures.	☑	☐	☐	☐	☐
	Applicability Notes This requirement applies to keys used to encrypt stored account data and to keyencrypting keys used to protect data-encrypting keys. The requirement to protect keys used to protect stored account data from disclosure and misuse applies to both data-encrypting keys and key-encrypting keys. Because one keyencrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures.						
3.6.1.2	Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times:	• Examine documented procedures. • Examine system configurations and key storage locations, including for keyencrypting keys.	☑	☐	☐	☐	☐

	• Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. • As at least two full-length key components or key shares, in accordance with an industry-accepted method. Applicability Notes It is not required that public keys be stored in one of these forms. Cryptographic keys stored as part of a key-management system (KMS) that employs SCDs are acceptable. A cryptographic key that is split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following: • Using an approved random number generator and within an SCD, OR • According to ISO 19592 or equivalent industry standard for generation of secret key shares.						
3.6.1.3	Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	• Examine user access lists.	☑	☐	☐	☐	☐
3.6.1.4	Cryptographic keys are stored in the fewest possible locations.	• Examine key storage locations. • Observe processes.	☑	☐	☐	☐	☐
3.7 Where cryptography is used to protect stored account data, key-management processes and procedures covering all aspects of the key lifecycle are defined and implemented.							

3.7.1	Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	• Examine documented key-management policies and procedures. • Observe the method for generating keys.	☑	☐	☐	☐	☐
3.7.2	Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	• Examine documented key-management policies and procedures. • Observe the method for distributing keys.	☑	☐	☐	☐	☐
3.7.3	Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	• Examine documented key-management policies and procedures. • Observe the method for storing keys.	☑	☐	☐	☐	☐
3.7.4	Key-management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod.	• Examine documented key-management policies and procedures. • Interview personnel. • Observe key storage locations.	☑	☐	☐	☐	☐
3.7.5			☑	☐	☐	☐	☐

	Key-management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	• Examine documented key-management policies and procedures. • Interview personnel.					
	Applicability Notes If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key).						
3.7.6	Where manual cleartext cryptographic key-management operations are performed by personnel, keymanagement policies and procedures are implemented include managing these operations using split knowledge and dual control.	• Examine documented key-management policies and procedures. • Interview personnel. • Observe processes.	☑	☐	☐	☐	☐
	Applicability Notes This control is applicable for manual key-management operations or where key management is not controlled by the encryption product. A cryptographic key that is simply split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following:						

	• Using an approved random number generator and within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-ofinteraction device, OR • According to ISO 19592 or equivalent industry standard for generation of secret key shares						
3.7.7	Key-management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	• Examine documented key-management policies and procedures. • Interview personnel. • Observe processes.	☑	☐	☐	☐	☐
3.7.8	Key-management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their keycustodian responsibilities.	• Examine documented key-management policies and procedures. • Review documentation or other evidence of key custodian acknowledgments.	☑	☐	☐	☐	☐

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

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 Tested	Not in Place
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented						
4.1.1 All security policies and operational procedures that are identified in Requirement 4 are: • Documented.	• Examine documentation. • Interview personnel.	☑	☐	☐	☐	☐

	• Kept up to date. • In use. • Known to all affected parties.						
4.1.2	Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel	☑	☐	☐	☐	☐
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						
	Only trusted keys and certificates are accepted.	• Examine documented policies and procedures. • Interview personnel. • Examine system configurations. • Examine cardholder data transmissions. • Examine keys and certificates.	☑	☐	☐	☐	☐
	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.		☐	☐	☑	☐	☐
	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.		☑	☐	☐	☐	☐
	The encryption strength is appropriate for the encryption methodology in use.		☑	☐	☐	☐	☐
	Applicability Notes						
	There could be occurrences where an entity receives cardholder data unsolicited via an insecure communication channel that was not intended for the purpose of receiving 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 implement measures to prevent the channel from being used for cardholder data. 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. Note that self-signed certificates where the Distinguished Name (DN) field in the "issued by" and "issued to" field is the same are not acceptable. 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						
4.2.1.1	An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.	• Examine documented policies and procedures. • Examine the inventory of trusted keys and certificates.	☐	☐	☑	☐	☐
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
4.2.1.2	Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	• Examine system configurations.	☑	☐	☐	☐	☐
4.2.2	PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.	• Examine documented policies and procedures. • Examine system configurations and vendor documentation.	☑	☐	☐	☐	☐
	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.					

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

Maintain a Vulnerability Management Program

Requirement 5: Protect All Systems and Networks from Malicious Software

PCI DSS Requirement		Expected Testing	Response: (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	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: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☑	☐	☐	☐	☐
5.1.2	Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood. New requirement - effective immediately	• Examine documentation. • Interview responsible personnel.	☑	☐	☐	☐	☐
5.2 Malicious software (malware) is prevented, or detected and addressed							
5.2.1	An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	• Examine system components. • Examine the periodic evaluations.	☑	☐	☐	☐	☐

5.2.2	The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	• Examine vendor documentation. • Examine system configurations.	☑	☐	☐	☐	☐
5.2.3	Any system components that are not at risk for malware are evaluated periodically to include the following: • 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.	• 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 antimalware solution deployed.	☑	☐	☐	☐	☐
	Applicability Notes						
	System components covered by this requirement are those for which there is no antimalware 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.	• Examine the targeted risk analysis. • Examine documented results of periodic evaluations. • Interview personnel.	☐	☐	☑	☐	☐
	Applicability Notes						

	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.							
5.3.1	The anti-malware solution(s) is kept current via automatic updates.	• Examine anti-malware solution(s) configurations, including any master installation. • Examine system components and logs.	☑	☐	☐	☐	☐
5.3.2	The anti-malware solution(s): • Performs periodic scans and active or real-time scans OR • Performs continuous behavioral analysis of systems or processes.	• Examine anti-malware solution(s) configurations, including any master installation. • Examine system components. • Examine logs and scan results.	☑	☐	☐	☐	☐
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.	• Examine the targeted risk analysis. • Examine documented results of periodic malware scans. • Interview personnel.	☐	☐	☑	☐	☐
	Applicability Notes						
	This requirement applies to entities conducting periodic malware scans to meet Requirement 5.3.2. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
5.3.3	For removable electronic media, the anti-malware solution(s):	• Examine anti-malware solution(s) configurations.	☐	☐	☑	☐	☐

	• Performs automatic scans of when the media is inserted, connected, or logically mounted, OR • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.	• Examine system components with removable electronic media. • Examine logs and scan results.					
	Applicability Notes This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
5.3.4	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	• Examine anti-malware solution(s) configurations.	☑	☐	☐	☐	☐
5.3.5	Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	• Examine anti-malware configurations. • Observe processes. • Interview responsible personnel.	☑	☐	☐	☐	☐
	Applicability Notes Anti-malware solutions may be temporarily disabled only if there is a legitimate technical need, as authorized by management on a case-by-case basis. If anti-malware protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which antimalware 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.	• Observe implemented processes. • Examine mechanisms.	☐	☐	☑	☐	☐

	Applicability Notes						
	This requirement applies to the automated mechanism. It is not intended that the systems and services providing such automated mechanisms (such as e-mail servers) are brought into scope for PCI DSS. The focus of this requirement is on protecting personnel with access to system components in-scope for PCI DSS. Meeting this requirement for technical and automated controls to detect and protect personnel against phishing is not the same as Requirement 12.6.3.1 for security awareness training. Meeting this requirement does not also meet the requirement for providing personnel with security awareness training, and vice versa. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						

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

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 Tested	Not in Place
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.							
6.1.1	All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties	• Examine documentation. • Interview personnel.	☑	☐	☐	☐	☐
6.1.2		• Examine documentation. • Interview responsible personnel.	☑	☐	☐	☐	☐

	Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.						
6.2 Bespoke and custom software are developed securely.							
6.2.1	Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle.	• Examine documented software development procedures.	☐	☐	☑	☐	☐
	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	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • 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.	• Examine documented software development procedures. • Examine training records. • Interview personnel.	☐	☐	☑	☐	☐

	Applicability Notes 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	Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines. • Code reviews look for both existing and emerging software vulnerabilities. • Appropriate corrections are implemented prior to release.	• Examine documented software development procedures. • Interview responsible personnel. • Examine evidence of changes to bespoke and custom software.	☐	☐	☑	☐	☐
	Applicability Notes This requirement for code reviews applies to all bespoke and custom software (both internal and public-facing), as part of the system development lifecycle. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.4. Code reviews may be performed using either manual or automated processes, or a combination of both.						
6.2.3.1	If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:	• Examine documented software development procedures. • Interview responsible personnel. • Examine evidence of changes to bespoke and custom software.	☐	☐	☑	☐	☐

	• 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.						
	Applicability Notes						
	Manual code reviews can be conducted by knowledgeable internal personnel or knowledgeable third-party personnel. 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.						
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						
	Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws	• Examine documented procedures. • Interview responsible software development personnel.	☐	☐	☑	☐	☐
	Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.		☐	☐	☑	☐	☐
	Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.		☐	☐	☑	☐	☐
			☐	☐	☑	☐	☐

	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).						
	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		☐	☐	☑	☐	☐
	Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.		☐	☐	☑	☐	☐
	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.						
6.3 Security vulnerabilities are identified and addressed.							
6.3.1	Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industryrecognized 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.	• Examine policies and procedures. • Interview responsible personnel. • Examine documentation. • Observe processes.	☑	☐	☐	☐	☐

	• Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. **Applicability Notes** This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.						
6.3.2	An inventory of bespoke and custom software, and thirdparty software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management. **Applicability Notes** This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment	• Examine documentation. • Interview personnel.	☐	☐	☑	☐	☐
6.3.3	All system components are protected from known vulnerabilities by installing applicable security patches /updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	• Examine policies and procedures. • Examine system components and related software. • Compare list of security patches installed to recent vendor patch lists.	☑	☐	☐	☐	☐

6.4 Public-facing web applications are protected against attacks.							

6.4.1	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows:
	• Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows:
	  • At least once every 12 months and after significant changes.
	  • By an entity that specializes in application security.
	  • Including, at a minimum, all common software attacks in Requirement 6.2.4.
	  • All vulnerabilities are ranked in accordance with Requirement 6.3.1.
	  • All vulnerabilities are corrected.
	  • The application is re-evaluated after the corrections OR
	• Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows:
	  • Installed in front of public-facing web applications to detect and prevent web-based attacks.
	  • Actively running and up to date as applicable.
	  • Generating audit logs.
	  • Configured to either block web-based attacks or generate an alert that is immediately investigated.
		• Examine documented processes.
		• Interview personnel.
		• Examine records of application security assessments
		• Examine the system configuration settings and audit logs.
			☑	☐	☐	☐	☐

	Applicability Notes This assessment is not the same as the vulnerability scans performed for Requirement 11.3.1 and 11.3.2. This requirement will be superseded by Requirement 6.4.2 after 31 March 2025 when Requirement 6.4.2 becomes effective.						
6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.	• Examine the system configuration settings. • Examine audit logs. • Interview responsible personnel.	☐	☐	☑	☐	☐
	Applicability Notes This new requirement will replace Requirement 6.4.1 once its effective date is reached. 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.						
6.4.3	All payment page scripts that are loaded and executed in the consumer's browser are managed as follows						
	A method is implemented to confirm that each script is authorized.	• Examine policies and procedures. • Interview responsible personnel. • Examine inventory records.	☐	☐	☑	☐	☐
			☐	☐	☑	☐	☐

	A method is implemented to assure the integrity of each script.	• Examine system configurations.					
	An inventory of all scripts is maintained with written justification as to why each is necessary.		☐	☐	☑	☐	☐
	Applicability Notes						
	This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties. 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.						
6.5 Changes to all system components are managed securely.							
6.5.1	Changes to all system components in the production environment are made according to established procedures that include: • 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.	• Examine documented change control procedures. • Examine recent changes to system components and trace changes to change control documentation. • Examine change control documentation.	☐	☐	☑	☐	☐
6.5.2	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.	• Examine documentation for significant changes. • Interview personnel. • Observe the affected systems /networks.	☐	☐	☑	☐	☐

	Applicability Notes These significant changes should also be captured and reflected in the entity's annual PCI DSS scope confirmation activity per Requirement 12.5.2						
6.5.3	Pre-production environments are separated from production environments and the separation is enforced with access controls.	• Examine policies and procedures. • Examine network documentation and configurations of network security controls. • Examine access control settings.	☐	☐	☑	☐	☐
6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.	• Examine policies and procedures. • Observe processes. • Interview personnel.	☐	☐	☑	☐	☐
	Applicability Notes In environments with limited personnel where individuals perform multiple roles or functions, this same goal can be achieved with additional procedural controls that provide accountability. For example, a developer may also be an administrator that uses an administrator-level account with elevated privileges in the development environment and, for their developer role, they use a separate account with user-level access to the production environment.						
6.5.5	Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.	• Examine policies and procedures. • Observe testing processes. • Interview personnel. • Examine pre-production test data.	☐	☐	☑	☐	☐
6.5.6	Test data and test accounts are removed from system components before the system goes into production.	• Examine policies and procedures.	☑	☐	☐	☐	☐

		• Observe testing processes for both offthe-shelf software and inhouse applications. • Interview personnel. • Examine data and accounts for recently installed or updated offthe-shelf software and inhouse applications.					

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

Implement Strong Access Control Measures

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

PCI DSS Requirement		Expected Testing	Response: (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.							
7.1.1	All security policies and operational procedures that are identified in Requirement 7 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☑	☐	☐	☐	☐
7.1.2	Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☑	☐	☐	☐	☐
7.2 Access to system components and data is appropriately defined and assigned.							
7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions.	• Examine documented policies and procedures. • Interview personnel. • Examine access control model settings.	☑	☐	☐	☐	☐

	• The least privileges required (for example, user, administrator) to perform a job function.						
7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.	• Examine policies and procedures. • Examine user access settings, including for privileged users. • Interview responsible management personnel. • Interview personnel responsible for assigning access.	☑	☐	☐	☐	☐
7.2.3	Required privileges are approved by authorized personnel	• Examine policies and procedures. • Examine user IDs and assigned privileges. • Examine documented approvals.	☑	☐	☐	☐	☐
7.2.4	All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • 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.	• Examine policies and procedures. • Interview responsible personnel. • Examine documented results of periodic reviews of user accounts.	☐	☐	☑	☐	☐

	Applicability Notes 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 thirdparty 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. 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.						
7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • 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.	• Examine policies and procedures. • Examine privileges associated with system and application accounts. • Interview responsible personnel.	☐	☐	☑	☐	☐
	Applicability Notes This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
7.2.5.1	All access by application and system accounts and related access privileges are reviewed as follows: • 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). • The application/system access remains appropriate for the function being performed. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	• Examine policies and procedures. • Examine the targeted risk analysis. • Interview responsible personnel. • Examine documented results of periodic reviews of system and application accounts and related privileges.	☐	☐	☑	☐	☐

	Applicability Notes This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment						
7.2.6	All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. • Only the responsible administrator(s) can directly access or query repositories of stored CHD.	• Examine policies and procedures. • Interview personnel. • Examine configuration settings for querying repositories of stored cardholder data	☑	☐	☐	☐	☐
	Applicability Notes This requirement applies to controls for user access to query repositories of stored cardholder data. 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.						
7.3 Access to system components and data is managed via an access control system(s).							
7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	• Examine vendor documentation. • Examine configuration settings.	☑	☐	☐	☐	☐
7.3.2	The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	• Examine vendor documentation. • Examine configuration settings.	☑	☐	☐	☐	☐
7.3.3		• Examine vendor documentation.	☑	☐	☐	☐	☐

	The access control system(s) is set to "deny all" by default.	• Examine configuration settings.					

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

Requirement 8: Identify Users and Authenticate Access to System Components

PCI DSS Requirement		Expected Testing	Response: (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.							
8.1.1	All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☑	☐	☐	☐	☐
8.1.2	Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☑	☐	☐	☐	☐
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.							
8.2.1	All users are assigned a unique ID before access to system components or cardholder data is allowed.	• Interview responsible personnel. • Examine audit logs and other evidence.	☑	☐	☐	☐	☐

	Applicability Notes This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).						
8.2.2	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.	• Examine user account lists on system components and applicable documentation. • Examine authentication policies and procedures. • Interview system administrators.	☑	☐	☐	☐	☐
	Applicability Notes This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).						
8.2.4	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval.	• Examine documented authorizations across various phases of the account lifecycle (additions, modifications, and deletions).	☑	☐	☐	☐	☐

	• Implemented with only the privileges specified on the documented approval. Applicability Notes This requirement applies to all user accounts, including employees, contractors, consultants, temporary workers, and third-party vendors.	• Examine system settings.					
8.2.5	Access for terminated users is immediately revoked.	• Examine information sources for terminated users. • Review current user access lists. • Interview responsible personnel.	☑	☐	☐	☐	☐
8.2.6	Inactive user accounts are removed or disabled within 90 days of inactivity.	• Examine user accounts and last logon information. • Interview responsible personnel.	☑	☐	☐	☐	☐
8.2.7	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: • Enabled only during the time period needed and disabled when not in use. • Use is monitored for unexpected activity.	• Interview responsible personnel. • Examine documentation for managing accounts. • Examine evidence.	☑	☐	☐	☐	☐
8.2.8	If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to reactivate the terminal or session.	• Examine system configuration settings.	☑	☐	☐	☐	☐

	Applicability Notes This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement is not meant to prevent legitimate activities from being performed while the console/PC is unattended.						
8.3 Strong authentication for users and administrators is established and managed							
8.3.1	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric element.	• Examine documentation describing the authentication factor(s) used. • For each type of authentication factor used with each type of system component, observe the authentication process.	☑	☐	☐	☐	☐
	Applicability Notes This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement does not supersede multi-factor authentication (MFA) requirements but applies to those in-scope systems not otherwise subject to MFA requirements. A digital certificate is a valid option for "something you have" if it is unique for a particular user						
8.3.2	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	• Examine vendor documentation • Examine system configuration settings. • Examine repositories of authentication factors. • Examine data transmissions.	☑	☐	☐	☐	☐

8.3.3	User identity is verified before modifying any authentication factor.	• Examine procedures for modifying authentication factors. • Observe security personnel.	☑	☐	☐	☐	☐
8.3.4	Invalid authentication attempts are limited by: • 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.	• Examine system configuration settings.	☑	☐	☐	☐	☐
	Applicability Notes This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).						
8.3.5	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use.	• Examine procedures for setting and resetting passwords /passphrases. • Observe security personnel.	☑	☐	☐	☐	☐
8.3.6		• Examine system configuration settings.	☑	☐	☐	☐	☐

	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters.						
	Applicability Notes This requirement is not intended to apply to: • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). • Application or system accounts, which are governed by requirements in section 8.6. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment. Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.						
8.3.7	Individuals are not allowed to submit a new password /passphrase that is the same as any of the last four passwords/passphrases used.	• Examine system configuration settings.	☑	☐	☐	☐	☐
	Applicability Notes This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).						
8.3.8	Authentication policies and procedures are documented and communicated to all users including:	• Examine procedures. • Interview personnel.	☑	☐	☐	☐	☐

	• 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.	• Review authentication policies and procedures that are distributed to users. • Interview users. ,					
8.3.9	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any singlefactor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. Applicability Notes This requirement applies to in-scope system components that are not in the CDE because these components are not subject to MFA requirements. This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement does not apply to service providers' customer accounts but does apply to accounts for service provider personnel.	• Inspect system configuration settings.	☑	☐	☐	☐	☐

8.3.11	Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.	• Examine authentication policies and procedures. • Interview security personnel. • Examine system configuration settings and/or observe physical controls, as applicable.	☑	☐	☐	☐	☐
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.							
8.4.1	MFA is implemented for all non-console access into the CDE for personnel with administrative access.	• Examine network and/or system configurations. • Observe administrator personnel logging into the CDE.	☑	☐	☐	☐	☐
	Applicability Notes						
	The requirement for MFA for non-console administrative access applies to all personnel with elevated or increased privileges accessing the CDE via a non-console connection- that is, via logical access occurring over a network interface rather than via a direct, physical connection. MFA is considered a best practice for non-console administrative access to in-scope system components that are not part of the CDE.						
8.4.2	MFA is implemented for all access into the CDE.	• Examine network and/or system configurations. • Observe personnel logging in to the CDE. • Examine evidence.	☐	☐	☑	☐	☐
	Applicability Notes						
	This requirement does not apply to:						

	• 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 (such as IDs used by cashiers on point-of-sale terminals). 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 via non-console administrative access from the entity's network into the CDE. 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. MFA for remote 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. 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.						
8.4.3	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: • All remote access by all personnel, both users and administrators, originating from outside the entity's network. • All remote access by third parties and vendors.	• Examine network and/or system configurations for remote access servers and systems. • Observe personnel (for example, users and administrators) connecting remotely to the network.	☑	☐	☐	☐	☐
	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. 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.						
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.							
8.5.1	MFA systems are implemented as follows: • 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.	• 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.	☐	☐	☑	☐	☐
	Applicability Notes This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
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: • Interactive use is prevented unless needed for an exceptional circumstance.	• Examine application and system accounts that can be used interactively. • Interview administrative personnel.	☐	☐	☑	☐	☐

	• 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.						
	Applicability Notes This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
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.	• 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.	☐	☐	☑	☐	☐
	Applicability Notes Stored passwords/passphrases are required to be encrypted in accordance with PCI DSS Requirement 8.3.2. 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.						
8.6.3		• Examine policies and procedures. • Examine the targeted risk analysis.	☐	☐	☑	☐	☐

	Passwords/passphrases for any application and system accounts are protected against misuse as follows: • 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.	• Interview responsible personnel. • Examine system configuration settings.					
	Applicability Notes This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						

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

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 Tested	Not in Place
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.							
9.1.1	All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date.	• Examine documentation. • Interview personnel.	☑	☐	☐	☐	☐

	• In use. • Known to all affected parties.						
9.1.2	Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	• Examine documentation. • Interview personnel.	☑	☐	☐	☐	☐
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.							
9.2.1	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	• Observe physical entry controls. • Interview responsible personnel.	☑	☐	☐	☐	☐
9.2.1.1	Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: • 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.	• 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.	☑	☐	☐	☐	☐
9.2.2		• Interview responsible personnel.	☑	☐	☐	☐	☐

	Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	• Observe locations of publicly accessible network jacks.					
9.2.3	Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	• Interview responsible personnel. • Observe locations of hardware and lines.	☑	☐	☐	☐	☐
9.2.4	Access to consoles in sensitive areas is restricted via locking when not in use.	• Observe a system administrator's attempt to log into consoles in sensitive areas.	☑	☐	☐	☐	☐
9.3 Physical access for personnel and visitors is authorized and managed.							
9.3.1	Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: • Identifying personnel. • Managing changes to an individual's physical access requirements. • Revoking or terminating personnel identification. • Limiting access to the identification process or system to authorized personnel.	• Examine documented procedures. • Observe identification methods, such as ID badges. • Observe processes.	☑	☐	☐	☐	☐
9.3.1.1	Physical access to sensitive areas within the CDE for personnel is controlled as follows:	• Observe personnel in sensitive areas within the CDE. • Interview responsible personnel.	☑	☐	☐	☐	☐

	• Access is authorized and based on individual job function. • Access is revoked immediately upon termination. • All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	• Examine physical access control lists. • Observe processes.					
9.3.2	Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel.	• Examine documented procedures. • Observe processes when visitors are present in the CDE. • Interview personnel. • Observe the use of visitor badges or other identification.	☑	☐	☐	☐	☐
9.3.3	Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.	• Observe visitors leaving the facility • Interview personnel.	☑	☐	☐	☐	☐
9.3.4	A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit.	• Examine the visitor log. • Interview responsible personnel. • Examine visitor log storage locations.	☑	☐	☐	☐	☐

	• The name of the personnel authorizing physical access. • Retaining the log for at least three months, unless otherwise restricted by law.						
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.							
9.4.1	All media with cardholder data is physically secured.	• Examine documentation.	☑	☐	☐	☐	☐
9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	• Examine documented procedures. • Examine logs or other documentation. • Interview responsible personnel at the storge location(s).	☑	☐	☐	☐	☐
9.4.1.2	The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	• Examine documented procedures, logs, or other documentation. • Interview responsible personnel at the storage location(s).	☑	☐	☐	☐	☐
9.4.2	All media with cardholder data is classified in accordance with the sensitivity of the data.	• Examine documented procedures. • Examine media logs or other documentation.	☑	☐	☐	☐	☐
9.4.3	Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged.	• Examine documented procedures. • Interview personnel. • Examine records. • Examine offsite tracking logs for all media.	☑	☐	☐	☐	☐

	• Media is sent by secured courier or other delivery method that can be accurately tracked. • Offsite tracking logs include details about media location.						
9.4.4	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals). Applicability Notes Individuals approving media movements should have the appropriate level of management authority to grant this approval. However, it is not specifically required that such individuals have "manager" as part of their title.	• Examine documented procedures. • Examine offsite media tracking logs. • Interview responsible personnel.	☑	☐	☐	☐	☐
9.4.5	Inventory logs of all electronic media with cardholder data are maintained.	• Examine documented procedures. • Examine electronic media inventory logs. • Interview responsible personnel.	☑	☐	☐	☐	☐
9.4.5.1	Inventories of electronic media with cardholder data are conducted at least once every 12 months.	• Examine documented procedures. • Examine electronic media inventory logs. • Interview responsible personnel.	☑	☐	☐	☐	☐
9.4.6	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows:	• Examine the periodic media destruction policy. • Observe processes. • Interview personnel.	☑	☐	☐	☐	☐

	• 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.	• Observe storage containers.					
	Applicability Notes These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.						
9.4.7	Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed.	• Examine the periodic media destruction policy. • Observe the media destruction process. • Interview responsible personnel.	☑	☐	☐	☐	☐
	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.						
9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.							
9.5.1		• Examine documented policies and procedures.	☐	☐	☑	☐	☐

	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: • 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.						
	Applicability Notes 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). This requirement is not intended to apply to manual PAN key-entry components such as computer keyboards. This requirement is recommended, but not required, for manual PAN key-entry components such as computer keyboards. This requirement does not apply to commercial off-the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution.						
9.5.1.1	An up-to-date list of POI devices is maintained, including: • Make and model of the device. • Location of device. • Device serial number or other methods of unique identification.	• Examine the list of POI devices. • Observe POI devices and device locations. • Interview personnel.	☐	☐	☑	☐	☐
9.5.1.2		• Examine documented procedures.	☐	☐	☑	☐	☐

	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	• Interview responsible personnel. • Observe inspection processes.					
9.5.1.2.1	The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. Applicability Notes This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.	• Examine the targeted risk analysis. • Examine documented results of periodic device inspections. • Interview personnel.	☐	☐	☑	☐	☐
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: • 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.	• Review training materials for personnel in POI environments. • Interview responsible personnel.	☐	☐	☑	☐	☐

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

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 Tested	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: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☑	☐	☐	☐	☐
10.1.2	Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☑	☐	☐	☐	☐
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.							
10.2.1	Audit logs are enabled and active for all system components and cardholder data.	• Interview the system administrator. • Examine system configurations	☑	☐	☐	☐	☐
10.2.1.1	Audit logs capture all individual user access to cardholder data.	• Examine audit log configurations. • Examine audit log data.	☑	☐	☐	☐	☐

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.	• Examine audit log configurations. • Examine audit log data.	☑	☐	☐	☐	☐
10.2.1.3	Audit logs capture all access to audit logs.	• Examine audit log configurations. • Examine audit log data.	☑	☐	☐	☐	☐
10.2.1.4	Audit logs capture all invalid logical access attempts.	• Examine audit log configurations. • Examine audit log data.	☑	☐	☐	☐	☐
10.2.1.5	Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.	• Examine audit log configurations. • Examine audit log data.	☑	☐	☐	☐	☐
10.2.1.6	Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs.	• Examine audit log configurations. • Examine audit log data.	☑	☐	☐	☐	☐

10.2.1.7	Audit logs capture all creation and deletion of system-level objects.	• Examine audit log configurations. • Examine audit log data.	☑	☐	☐	☐	☐
10.2.2	Audit logs record the following details for each auditable event: • 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).	• Interview responsible personnel. • Examine audit log configurations. • Examine audit log data.	☑	☐	☐	☐	☐
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.	• Interview system administrators • Examine system configurations and privileges.	☑	☐	☐	☐	☐
10.3.2	Audit log files are protected to prevent modifications by individuals.	• Examine system configurations and privileges. • Interview system administrators.	☑	☐	☐	☐	☐
10.3.3	Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	• Examine backup configurations or log files.	☑	☐	☐	☐	☐

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.	• Examine system settings. • Examine monitored files. • Examine results from monitoring activities.	☑	☐	☐	☐	☐
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.							
10.4.1	The following audit logs are reviewed at least once daily: • 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).	• Examine security policies and procedures. • Observe processes. • Interview personnel.	☑	☐	☐	☐	☐
10.4.1.1	Automated mechanisms are used to perform audit log reviews.	• Examine log review mechanisms. • Interview personnel	☐	☐	☑	☐	☐
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
10.4.2		• Examine security policies and procedures.	☑	☐	☐	☐	☐

	Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.	• Examine documented results of log reviews. • Interview personnel.					
	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.	• Examine the targeted risk analysis. • Examine documented results of periodic log reviews. • Interview personnel.	☐	☐	☑	☐	☐
	Applicability Notes This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
10.4.3	Exceptions and anomalies identified during the review process are addressed.	• Examine security policies and procedures. • Observe processes. • Interview personnel.	☑	☐	☐	☐	☐
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.	• Examine documented audit log retention policies and procedures. • Examine configurations of audit log history. • Examine audit logs. • Interview personnel. • Observe processes.	☑	☐	☐	☐	☐

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. 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.	• Examine system configuration settings.	☑	☐	☐	☐	☐
10.6.2	Systems are configured to the correct and consistent time as follows: • 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).	• Examine system configuration settings for acquiring, distributing, and storing the correct time.	☑	☐	☐	☐	☐
10.6.3	Time synchronization settings and data are protected as follows:	• Examine system configurations and time-synchronization settings and logs.	☑	☐	☐	☐	☐

	• 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.	• Observe processes.					
10.7 Failures of critical security control systems are detected, reported, and responded to promptly							
10.7.2	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • Change-detection mechanisms. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used).	• Examine documented processes. • Observe detection and alerting processes. • Interview personnel.	☐	☐	☑	☐	☐
	Applicability Notes This requirement applies to all entities, including service providers, and will supersede Requirement 10.7.1 as of 31 March 2025. It includes two additional critical security control systems not in Requirement 10.7.1. 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.						
10.7.3	Failures of any critical security controls systems are responded to promptly, including but not limited to:	• Examine documented processes. • Interview personnel.	☑	☐	☐	☐	☐

	• Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls.	• Examine records related to critical security control systems failures.					
	Applicability Notes						
	This requirement applies only when the entity being assessed is a service provider until 31 March 2025, after which this requirement will apply to all entities. This is a current v3.2.1 requirement that applies to service providers only. However, this requirement is a best practice for all other entities until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						

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

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 Tested	Not in Place
11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.						
11.1.1 All security policies and operational procedures that are identified in Requirement 11 are:	• Examine documentation. • Interview personnel.	☑	☐	☐	☐	☐

	• Documented. • Kept up to date. • In use. • Known to all affected parties.						
11.1.2	Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☑	☐	☐	☐	☐
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.							
11.2.1	Authorized and unauthorized wireless access points are managed as follows: • 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.	• Examine policies and procedures. • Examine the methodology(ies) in use and the resulting documentation. • Interview personnel. • Examine wireless assessment results. • Examine configuration settings.	☑	☐	☐	☐	☐
	Applicability Notes The requirement applies even when a policy exists that prohibits the use of wireless technology since attackers do not read and follow company policy. 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.						

11.2.2	An inventory of authorized wireless access points is maintained, including a documented business justification.	• Examine documentation.	☑	☐	☐	☐	☐
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.							
11.3.1	Internal vulnerability scans are performed as follows: • At least once every three months. • High-risk and critical vulnerabilities (per 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	• Examine internal scan report results. • Examine scan tool configurations. • Interview responsible personne	☑	☐	☐	☐	☐
	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.						
11.3.1.1	All other applicable vulnerabilities (those not ranked as high-risk or critical (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows:	• Examine the targeted risk analysis. • Interview responsible personnel. • Examine internal scan report results or other documentation.	☐	☐	☑	☐	☐

	• Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. • Rescans are conducted as needed.						
	Applicability Notes						
	The timeframe for addressing lower-risk vulnerabilities is subject to the results of a risk analysis per Requirement 12.3.1 that includes (minimally) identification of assets being protected, threats, and likelihood and/or impact of a threat being realized. 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.						
11.3.1.2	Internal vulnerability scans are performed via authenticated scanning as follows						
	Systems that are unable to accept credentials for authenticated scanning are documented.	• Examine documentation. • Examine scan tool configurations. • Examine scan report results. • Interview personnel. • Examine accounts used for authenticated scanning.	☐	☐	☑	☐	☐
	Sufficient privileges are used for those systems that accept credentials for scanning.		☐	☐	☑	☐	☐
	If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.		☐	☐	☑	☐	☐
	Applicability Notes						
	The authenticated scanning tools can be either host-based or network-based. "Sufficient" privileges are those needed to access system resources such that a thorough scan can be conducted that detects known vulnerabilities. This requirement does not apply to system components that cannot accept credentials for scanning. Examples of systems that may not accept credentials for scanning include some network and security appliances, mainframes, and containers. 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.						

11.3.1.3	Internal vulnerability scans are performed after any significant change as follows: • High-risk and critical vulnerabilities (per 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).	• Examine change control documentation. • Interview personnel. • Examine internal scan and rescan report as applicable. • Interview personnel.	☑	☐	☐	☐	☐
	Applicability Notes Authenticated internal vulnerability scanning per Requirement 11.3.1.2 is not required for scans performed after significant changes.						
11.3.2	External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor (ASV) • Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	• Examine ASV scan reports.	☑	☐	☐	☐	☐
	Applicability Notes For initial PCI DSS compliance, 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). However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred. 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. Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.						
11.3.2.1	External vulnerability scans are performed after any significant change as follows: • 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).	• Examine change control documentation. • Interview personnel. • Examine external scan, and as applicable rescan reports.	☑	☐	☐	☐	☐
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.							
11.4.1	A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scopereduction controls.	• Examine documentation. • Interview personnel.	☑	☐	☐	☐	☐

	• Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities results for at least 12 months.						
	Applicability Notes Testing from inside the network (or "internal penetration testing") means testing from both inside the CDE and into the CDE from trusted and untrusted internal networks. Testing from outside the network (or "external penetration testing") means testing the exposed external perimeter of trusted networks, and critical systems connected to or accessible to public network infrastructures.						
11.4.2	Internal penetration testing is performed: • Per the entity's defined methodology. • At least once every 12 months. • After any significant infrastructure or application upgrade or change. • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV).	• Examine scope of work. • Examine results from the most recent external penetration test. • Interview responsible personnel.	☑	☐	☐	☐	☐

11.4.3	External penetration testing is performed: • Per the entity's defined methodology. • At least once every 12 months. • After any significant infrastructure or application upgrade or change. • By a qualified internal resource or qualified external third-party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	• Examine scope of work. • Examine results from the most recent external penetration test. • Interview responsible personnel.	☑	☐	☐	☐	☐
11.4.4	Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.	• Examine penetration testing results.	☑	☐	☐	☐	☐
11.4.5	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods	• Examine segmentation controls. • Review penetration-testing methodology. • Examine the results from the most recent penetration test.	☑	☐	☐	☐	☐

	• Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • 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).	• Interview responsible personnel.					
11.5 Network intrusions and unexpected file changes are detected and responded to.							
11.5.1	Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	• Examine system configurations and network diagrams. • Examine system configurations. • Interview responsible personnel. • Examine vendor documentation.	☑	☐	☐	☐	☐
11.5.2	A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows:	• Examine system settings for the change-detection mechanism. • Examine monitored files.	☑	☐	☐	☐	☐

	• To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.	• Examine results from monitoring activities.					
	Applicability Notes						
	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).						
11.6 Unauthorized changes on payment pages are detected and responded to							
11.6.1	A change- and tamper-detection mechanism is deployed as follows						
	To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.	• Examine system settings and mechanism configuration settings. • Examine monitored payment pages. • Examine results from monitoring activities. • Examine the mechanism configuration settings. • Examine configuration settings. • Interview responsible personnel. • If applicable, examine the targeted risk analysis.	☐	☐	☑	☐	☐
	The mechanism is configured to evaluate the received HTTP header and payment page.		☐	☐	☑	☐	☐
	The mechanism functions are performed as follows: • At least once every seven days OR		☐	☐	☑	☐	☐

	• 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).						
	Applicability Notes						
	The intention of this requirement is not that an entity install software in the systems or browsers of its consumers, but rather that the entity uses techniques such as those described under Examples in the PCI DSS Guidance column to prevent and detect unexpected script activities. 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.						

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

Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs

PCI DSS Requirement		Expected Testing	Response: (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.							
12.1.1	An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	• Examine the information security policy. • Interview personnel.	☑	☐	☐	☐	☐
12.1.2	The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment	• Examine the information security policy. • Interview responsible personnel.	☑	☐	☐	☐	☐
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.	• Examine the information security policy. • Interview responsible personnel. • Examine documented evidence.	☑	☐	☐	☐	☐

12.1.4	Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.	• Examine the information security policy.	☑	☐	☐	☐	☐
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: • Explicit approval by authorized parties. • Acceptable uses of the technology. • List of products approved by the company for employee use, including hardware and software.	• Examine acceptable use policies. • Interview responsible personnel.	☑	☐	☐	☐	☐
	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.						
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.							
12.3.1	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against.	• Examine documented policies and procedures.	☐	☐	☑	☐	☐

	• 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 frequently the requirement must be performed to minimize the likelihood 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.						
	Applicability Notes This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
12.3.3	Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.	• Examine documentation. • Interview personnel.	☐	☐	☑	☐	☐

	Applicability Notes The requirement applies to all cryptographic suites and protocols used to meet PCI DSS requirements. 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.						
12.3.4	Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.	• Examine documentation. • Interview personnel.	☐	☐	☑	☐	☐
	Applicability Notes This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment						
12.5 PCI DSS scope is documented and validated.							
12.5.1	An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.	• Examine the inventory. • Interview personnel.	☑	☐	☐	☐	☐

12.5.2	PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes						
	PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment.	• Examine documented results of scope reviews. • Interview personnel (12.5.2 Only).	☑	☐	☐	☐	☐
	Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce).		☑	☐	☐	☐	☐
	Updating all data-flow diagrams per requirement 1.2.4.		☑	☐	☐	☐	☐
	Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups.		☑	☐	☐	☐	☐
	Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE.		☑	☐	☐	☐	☐
	Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.		☑	☐	☐	☐	☐
	Identifying all connections from third-party entities with access to the CDE.		☑	☐	☐	☐	☐

	Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope. Applicability Notes This annual confirmation of PCI DSS scope is an activity expected to be performed by the entity under assessment, and is not the same, nor is it intended to be replaced by, the scoping confirmation performed by the entity's assessor during the annual assessment.		☑	☐	☐	☐	☐
12.6 Security awareness education is an ongoing activity.							
12.6.1	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	• Examine the security awareness program.	☑	☐	☐	☐	☐
12.6.2	The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data. Applicability Notes This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.	• Examine security awareness program content. • Examine evidence of reviews. • Interview personnel.	☐	☐	☑	☐	☐
12.6.3	Personnel receive security awareness training as follows:	• Examine security awareness program records. • Interview applicable personnel.	☑	☐	☐	☐	☐

	• Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	• Examine the security awareness program materials. • Examine personnel acknowledgements.					
12.6.3.1	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: • Phishing and related attacks. • Social engineering. Applicability Notes See Requirement 5.4.1 in PCI DSS for guidance on the difference between technical and automated controls to detect and protect users from phishing attacks, and this requirement for providing users security awareness training about phishing and social engineering. These are two separate and distinct requirements, and one is not met by implementing controls required by the other one. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.	• Examine security awareness training content.	☐	☐	☑	☐	☐
12.6.3.2	Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1. Applicability Notes This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.	• Examine security awareness training content.	☐	☐	☑	☐	☐

12.7 Personnel are screened to reduce risks from insider threats.							
12.7.1	Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources. Applicability Notes For those potential personnel to be hired for positions such as store cashiers, who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	• Interview responsible Human Resource department management personnel.	☑	☐	☐	☐	☐
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. 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.	• Examine policies and procedures. • Examine list of TPSPs.	☑	☐	☐	☐	☐
12.8.2	Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	• Examine policies and procedures. • Examine written agreements with TPSPs.	☑	☐	☐	☐	☐

	Applicability Notes The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgment does not have to include the exact wording provided in this requirement. Evidence that a TPSP is meeting PCI DSS requirements (for example, a PCI DSS Attestation of Compliance (AOC) or a declaration on a company's website) is not the same as a written agreement specified in this requirement.						
12.8.3	An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	• Examine policies and procedures. • Examine evidence. • Interview responsible personnel.	☑	☐	☐	☐	☐
12.8.4	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	☑	☐	☐	☐	☐
	Applicability Notes Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for example, via a firewall service), the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also "not in place" for the entity.						
12.8.5	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	☑	☐	☐	☐	☐

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.							
12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • 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.	• Examine the incident response plan. • Interview personnel. • Examine documentation from previously reported incidents.	☑	☐	☐	☐	☐
12.10.2	At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1.	• Interview personnel. • Examine documentation.	☑	☐	☐	☐	☐
12.10.3		• Interview responsible personnel.	☑	☐	☐	☐	☐

	Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.	• Examine documentation.					
12.10.4	Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.	• Interview incident response personnel. • Examine training documentation.	☑	☐	☐	☐	☐
12.10.4.1	The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. Applicability Notes This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.	• Examine the targeted risk analysis.	☐	☐	☑	☐	☐
12.10.5	The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Detection of unauthorized wireless access points.	• Examine documentation. • Observe incident response processes.	☑	☐	☐	☐	☐

	Applicability Notes The bullet above (for monitoring and responding to alerts from a change- and tamperdetection mechanism for payment pages) is a best practice until 31 March 2025, after which it will be required as part of Requirement 12.10.5 and must be fully considered during a PCI DSS assessment.						
12.10.6	The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	• Examine policies and procedures. • Examine the security incident response plan. • Interview responsible personnel.	☑	☐	☐	☐	☐
12.10.7	Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected.	• Examine documented incident response procedures. • Interview personnel. • Examine records of response actions.	☐	☐	☑	☐	☐
	Applicability Notes						

	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.					

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

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 Tested	Not in Place
A2.1 POI terminals using SSL and/or early TLS are not susceptible to known SSL/TLS exploits							
A2.1.1	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.	• 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	☐	☐	☑	☐	☐
	Applicability Notes						
	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. 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.						

Appendix A3: Designated Entities Supplemental Validation (DESV)

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

Appendix B: Compensating Controls Worksheet

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

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

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

Requirement Number and Definition:

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

Appendix C: Explanation of Requirements Noted as Not Applicable

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

Requirement	Reason Requirement is Not Applicable
Example:	
Requirement 3.5.1	Account data is never stored electronically
Requirement 3.3.2	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 3.4.2	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 3.5.1.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 3.5.1.2	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 3.5.1.3	RMG does not use Disk Encryption
Requirement 4.2.1.b	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 4.2.1.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 5.2.3.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 5.3.2.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 5.3.3	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Requirement 5.4.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 6.2.1	Custom code is not currently completed on a PCI related system.
Requirement 6.2.2	Custom code is not currently completed on a PCI related system.
Requirement 6.2.3	Custom code is not currently completed on a PCI related system.
Requirement 6.2.3.1	Custom code is not currently completed on a PCI related system.
Requirement 6.2.4.a	Custom code is not currently completed on a PCI related system.
Requirement 6.2.4.b	Custom code is not currently completed on a PCI related system.
Requirement 6.2.4.c	Custom code is not currently completed on a PCI related system.
Requirement 6.2.4.d	Custom code is not currently completed on a PCI related system.
Requirement 6.2.4.e	Custom code is not currently completed on a PCI related system.

Requirement 6.2.4.f	Custom code is not currently completed on a PCI related system.
Requirement 6.3.2	This question is specific to the development of custom web applications and only needs to be answered if you write your own custom web applications. You have indicated in your profile that you do not write your own custom web applications.
Requirement 6.4.2	This question is specific to the development of custom web applications and only needs to be answered if you write your own custom web applications. You have indicated in your profile that you do not write your own custom web applications.
Requirement 6.4.3.a	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 6.4.3.b	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 6.4.3.c	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 6.5.1	Custom code is not currently completed on a PCI related system.
Requirement 6.5.2	Custom code is not currently completed on a PCI related system.
Requirement 6.5.3	Custom code is not currently completed on a PCI related system.
Requirement 6.5.4	Custom code is not currently completed on a PCI related system.

Requirement 6.5.5	Custom code is not currently completed on a PCI related system.
Requirement 7.2.4	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 7.2.5	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 7.2.5.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 8.4.2	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 8.5.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 8.6.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 8.6.2	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 8.6.3	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 9.5.1	POI devices are not used

Requirement 9.5.1.1	POI devices are not used
Requirement 9.5.1.2	POI devices are not used
Requirement 9.5.1.2.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 9.5.1.3	POI devices are not used
Requirement 10.4.1.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 10.4.2.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 10.7.2	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 11.3.1.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 11.3.1.2.a	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 11.3.1.2.b	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Requirement 11.3.1.2.c	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 11.6.1.a	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 11.6.1.b	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 11.6.1.c	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 12.3.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 12.3.3	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 12.3.4	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 12.6.2	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 12.6.3.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 12.6.3.2	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Requirement 12.10.4.1	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement 12.10.7	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
Requirement A2.1.1	POI devices are not used

Appendix D: Explanation of Requirements Noted as Not Tested

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

Requirement	Description of Requirement(s) Not Tested	Describe why Requirement(s) was Excluded from the Assessment
Examples:		
Requirement 10	No requirements from Requirement 10 were tested.	This assessment only covers requirements in Milestone 1 of the Prioritized Approach.
Requirements 1-8, 10-12	Only Requirement 9 was reviewed for this assessment. All other requirements were excluded.	Company is a physical hosting provider (CO-LO), and only physical security controls were considered for this assessment.

Annotation

MIDs/ Accounts covered by this Attestation-of-Compliance

Mid / Account	Company name	Address Line 1
240581627	Moore Response	100 Jamison Court, Hagerstown, Maryland, 21740

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation:

This AOC is based on results noted in SAQ D (Section 2) dated 03/04/2024.

Indicate below whether a full or partial PCI DSS assessment was completed:

- ☐ **Full** - All requirements have been assessed therefore no requirements were marked as Not Tested in the SAQ.
- ☐ **Partial** - One or more requirements have not been assessed and were therefore marked as Not Tested in the SAQ. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the SAQ D 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:

[x]	**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 Moore Response has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.
[ ]	**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 Moore Response has not demonstrated compliance with the PCI DSS requirements included in this SAQ. **Target Date** for Compliance: A merchant submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
[ ]	**Compliant but with Legal exception:** One or more assessed 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 Moore Response has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. If selected, complete the following:

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

Part 3a. Merchant Acknowledgement

Signatory(s) confirms:
(Select all that apply)

x	PCI DSS Self-Assessment Questionnaire D , Version 4.0, was completed according to the instructions therein.
x	All information within the above-referenced SAQ and in this attestation fairly represents the results of the merchant's assessment in all material respects.
x	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 This was electronically signed by 240581627 on behalf of Moore Response	*Date:* 03/04/2024
Merchant Executive Officer Name: Jeff Myland DocuSigned by: Jeffrey R Myland, CIO F3D3234E0D28465...	*Title:* Chief Information Officer

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this assessment, indicate the role performed: QSA not required per PCI requirements.	☐ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:
Signature of Lead QSA	*Date:*
Lead QSA Name:	
Signature of Duly Authorized Officer of QSA Company	*Date:*
Duly Authorized Officer Name:	*QSA Company:*

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

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

Part 4. Action Plan for Non-Compliant Requirements

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

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

PCI DSS Requirement*	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Log and monitor all access to system components and cardholder data	☐	☐	
11	Test security of systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	
Appendix.A2	Additional PCI DSS Requirements for Entities using SSL /Early TLS for Card-Present POS POI Terminal Connections	☐	☐