# Payment Card Industry
# Data Security Standard

## Self-Assessment Questionnaire D for Service Providers and Attestation of Compliance

### For use with PCI DSS Version 4.0.1

Revision 2

Publication Date: January 2025

# 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.<br>Rearranged, retitled, and expanded information in the "Completing the Self-Assessment Questionnaire" section (previously titled "Before You Begin").<br>Aligned content in Sections 1 and 3 of Attestation of Compliance (AOC) with PCI DSS v4.0 Report on Compliance AOC.<br>Added Section 2a to the Self-Assessment Questionnaire to specify additional documentation required for service provider self-assessments.<br>Added "Describe Results" to Section 2b (previously Section 2) for each PCI DSS requirement, for service providers to describe their testing results.<br>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.<br>Added "In Place with CCW" to AOC Section 3.<br>Added guidance for responding to future-dated requirements.<br>Added minor clarifications and addressed typographical errors. |
| May 2023 | 4.0 | 2 | Errata Change – Unlocked document in Section 2a to allow diagrams to be added. |
| August 2023 | 4.0 | 3 | Updated AOC Part 2g to include a section to explain Not Tested and Not Applicable reporting responses. |
| October 2024 | 4.0.1 | | Updated to align with PCI DSS v4.0.1. For details of PCI DSS changes, see *PCI DSS – Summary of Changes from PCI DSS v4.0 to 4.0.1.*<br>Added ASV Resource Guide to section "Additional PCI SSC Resources." |
| December 2024 | 4.0.1 | 1 | Errata Change – Corrected requirement number reference in Requirement 3.6.1.1. |
| January 2025 | 4.0.1 | 2 | Errata Change – In Document Changes table, updated November 2024 date in to reflect the December change date. Fixed Table of Contents so it is clickable. |

# Contents

# Completing the Self-Assessment Questionnaire

## Service Provider Eligibility Criteria for Self-Assessment Questionnaire D

Self-Assessment Questionnaire (SAQ) D for Service Providers applies to all service providers defined by a payment brand as being eligible to complete a self-assessment questionnaire.

***This SAQ is the ONLY SAQ option for 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 cardholder data and/or sensitive authentication data. Cardholder data and sensitive authentication data are considered account data and are defined as follows:

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

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

## PCI DSS Self-Assessment Completion Steps

1. Per the eligibility criteria in this SAQ and as spelled out in the *Self-Assessment Questionnaire Instructions and Guidelines* document on PCI SSC website, *this SAQ is the ONLY SAQ OPTION for service providers*.
2. Confirm that the service provider environment is properly scoped.
3. Assess 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:
     - 2a – Details about Reviewed Environment.
     - 2b – Self-Assessment Questionnaire D for Service Providers.
   - 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 an entity is expected to perform to verify that a requirement has been met.

The intent behind each testing method is described as follows:

- Examine: The entity critically evaluates data evidence. Common examples include documents (electronic or physical), screenshots, configuration files, audit logs, and data files.
- Observe: The entity 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 entity 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 entity 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 entity's particular implementation.

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

## Requirement Responses

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

A description of the meaning for each response and how to report the testing performed is provided in the table below:

| Response | When to use this response: | Service Provider Required Reporting |
|---|---|---|
| **In Place** | The expected testing has been performed, and all elements of the requirement have been met as stated. | Briefly describe how the testing and evidence demonstrates the requirement is In Place. |
| **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. | Briefly describe which aspect(s) of the requirement where a compensating control(s) was used.<br>All responses in this column also require completion of a Compensating Controls Worksheet (CCW) in Appendix B of this SAQ.<br>Information on the use of compensating controls and guidance on how to complete the CCW is provided in PCI DSS Appendices B and C. |
| **Not Applicable** | The requirement does not apply to the entity's environment. (See "Guidance for Not Applicable Requirements" below for examples.) | Briefly describe the results of testing performed that demonstrate the requirement is Not Applicable.<br>All responses in this column also 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.) | Briefly describe why this requirement was excluded from the assessment.<br>All responses in this column also 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 entity can confirm they are in place. This response is also used if a requirement cannot be met due to a legal restriction. (See "Legal Exception" below for more guidance). | Briefly describe how the testing and evidence demonstrates the requirement is Not in Place.<br>Responses in this column may require the completion of Part 4, if requested by the entity to which this SAQ will be submitted.<br>If the requirement is not in place due to a legal restriction, describe the statutory law or regulation that prohibits the requirement from being met and complete the relevant attestation in Part 3 of this SAQ. |

### *Guidance for Not Applicable Requirements*

While many entities 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 an entity to select "Not Applicable" for Requirements 1.3.3, 2.3.1, 2.3.2, and 4.2.1.2, the entity first needs to confirm that there are no wireless technologies used in their cardholder data environment (CDE) or that connect to their CDE. Once this has been confirmed, the organization 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 response should be selected. Examples of situations where this could occur include:

- An entity is asked by their acquirer to validate a subset of requirements—for example, using the PCI DSS Prioritized Approach to validate only certain milestones.
- An entity 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.
- A service provider organization offers a service which covers only a limited number of PCI DSS requirements—for example, a physical storage provider that is only confirming the physical security controls per PCI DSS Requirement 9 for their storage facility.

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

If any requirements are completely excluded from the entity'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 entity 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 PCI DSS requirement or bullet with an extended implementation period includes the following note: "*This requirement [or bullet] is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*"

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

### *Legal Exception*

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

***Note:*** *A legal exception is a legal restriction due to a local or regional law, regulation, or regulatory requirement, where meeting a PCI DSS requirement would violate that law, regulation, or regulatory requirement.*

*Contractual obligations or legal advice are not legal restrictions.*

### *Use of the Customized Approach*

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

*Use of the Customized Approach is not supported in SAQs.*

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

## Additional PCI SSC Resources

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

| Resource | Includes: |
|---|---|
| PCI DSS<br>*(PCI Data Security Standard Requirements and Testing Procedures)* | ▪ Guidance on Scoping<br>▪ Guidance on the intent of all PCI DSS Requirements<br>▪ Details of testing procedures<br>▪ Guidance on Compensating Controls<br>▪ Appendix G: Glossary of Terms, Abbreviations, and Acronyms |
| SAQ Instructions and Guidelines | ▪ Information about all SAQs and their eligibility criteria<br>▪ 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:<br>– *Understanding PCI DSS Scoping and Network Segmentation*<br>– *Third-Party Security Assurance*<br>– *Multi-Factor Authentication Guidance*<br>– *Best Practices for Maintaining PCI DSS Compliance* |
| Getting Started with PCI | ▪ Resources for smaller merchants including:<br>– *Guide to Safe Payments*<br>– *Common Payment Systems*<br>– *Questions to Ask Your Vendors*<br>– *Glossary of Payment and Information Security Terms*<br>– *PCI Firewall Basics*<br>– *ASV Resource Guide* |

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 entity's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures.* Complete all sections: The entity 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 Entity** | |
| Company name: | Paritor Ltd |
| DBA (doing business as): | |
| Company mailing address: | 19 Knowle Village, Budleigh Salterton, Devon, EX9 6AL |
| Company main website: | https://www.paritor.com |
| Company contact name: | Simon Dutton |
| Company contact title: | Mr |
| Contact phone number: | +44 1392 304150 |
| Contact e-mail address: | Simon@paritor.co.uk |

| **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. Scope Verification

**Services that were INCLUDED in the scope of the PCI DSS Assessment** (select all that apply):

| Name of service(s) assessed: | Xperios | |
|---|---|---|
| Type of service(s) assessed: | | |
| **Hosting Provider:**<br>☒ Applications / software<br>☐ Hardware<br>☐ Infrastructure / Network<br>☐ Physical space (co-location)<br>☐ Storage<br>☐ Web-hosting services<br>☐ Security services<br>☐ 3-D Secure Hosting Provider<br>☐ Multi-Tenant Service Provider<br>☐ Other Hosting (specify): | **Managed Services:**<br>☐ Systems security services<br>☐ IT support<br>☐ Physical security<br>☐ Terminal Management System<br>☐ Other services (specify): | **Payment Processing:**<br>☐ POI / card present<br>☒ Internet / e-commerce<br>☐ MOTO / Call Center<br>☐ ATM<br>☐ Other processing (specify): |
| ☐ Account Management | ☐ Fraud and Chargeback | ☐ Payment Gateway/Switch |
| ☐ Back-Office Services | ☐ Issuer Processing | ☐ Prepaid Services |
| ☐ Billing Management | ☐ Loyalty Programs | ☐ Records Management |
| ☐ Clearing and Settlement | ☐ Merchant Services | ☐ Tax/Government Payments |
| ☐ Network Provider | | |
| ☐ Others (specify): | | |

***Note**: These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

## Part 2. Executive Summary *(continued)*

### Part 2a. Scope Verification *(continued)*

**Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment** (select all that apply):

| Name of service(s) not assessed: | |
|---|---|

Type of service(s) not assessed:

| **Hosting Provider:** | **Managed Services:** | **Payment Processing:** |
|---|---|---|
| ☐ Applications / software | ☐ Systems security services | ☐ POI / card present |
| ☐ Hardware | ☐ IT support | ☐ Internet / e-commerce |
| ☐ Infrastructure / Network | ☐ Physical security | ☐ MOTO / Call Center |
| ☐ Physical space (co-location) | ☐ Terminal Management System | ☐ ATM |
| ☐ Storage | ☐ Other services (specify): | ☐ Other processing (specify): |
| ☐ Web-hosting services | | |
| ☐ Security services | | |
| ☐ 3-D Secure Hosting Provider | | |
| ☐ Multi-Tenant Service Provider | | |
| ☐ Other Hosting (specify): | | |
| ☐ Account Management | ☐ Fraud and Chargeback | ☐ Payment Gateway/Switch |
| ☐ Back-Office Services | ☐ Issuer Processing | ☐ Prepaid Services |
| ☐ Billing Management | ☐ Loyalty Programs | ☐ Records Management |
| ☐ Clearing and Settlement | ☐ Merchant Services | ☐ Tax/Government Payments |
| ☐ Network Provider | | |
| ☐ Others (specify): | | |

| Provide a brief explanation why any checked services were not included in the assessment: | |
|---|---|

### Part 2b. Description of Role with Payment Cards

| Describe how the business stores, processes, and/or transmits account data. | We do not store, process or transmit account data |
|---|---|
| Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data. | Xperios provides a web portal that allows customers to select services and view/pay invoices. When a customer chooses to make a payment, the Xperios portal redirects the user to Pay360 using a secure, server to server handoff. All cardholder data entry, processing, and transmission occur entirely within Pay360's PCI compliant environment. Xperios does not receive, process, store, or transmit any cardholder data.<br><br>Our only involvement is initiating the redirect and receiving a post payment status response from Pay360. We cannot access or influence the customer's card data, but we do ensure |

| | |
|---|---|
| | that the redirection process is secure, that the Pay360 URL is correctly enforced, and that no card data can be entered into our systems. |
| Describe system components that could impact the security of account data. | The Xperios web portal and supporting backend services can indirectly impact the security of account data by controlling the initiation of the payment process. These components determine when a user is redirected to the Pay360 payment page and ensure that the redirect uses the correct, validated Pay360 URL.<br><br>Although Xperios does not store, process, or transmit any cardholder data, the following components could influence the security of the payment flow:<br><br>• Xperios Web Portal (frontend) – Presents invoice and service selection screens and triggers the redirect to Pay360. Must ensure no card data can be entered into Xperios forms.<br><br>• Backend Application Services – Generate the secure payment session request sent to Pay360 and validate the response after payment completion.<br><br>• Authentication & Session Management – Ensures only authorised users can initiate payments and prevents session tampering that could alter the redirect.<br><br>• Web Server / API Gateway – Enforces HTTPS, URL validation, and prevents modification of the Pay360 redirect endpoint.<br><br>• Configuration Management – Ensures the Pay360 endpoint, keys, and integration settings cannot be altered without authorisation.<br><br>• Logging & Monitoring Systems – Detect anomalies in the payment initiation flow (but never log card data).<br><br>These components do not handle account data directly, but they can affect the integrity and security of the redirection process that leads to Pay360's PCI compliant environment. |

## Part 2. Executive Summary *(continued)*

### Part 2c. Description of Payment Card Environment

| | |
|---|---|
| Provide a ***high-level*** description of the environment covered by this assessment.<br>*For example:*<br>• *Connections into and out of the cardholder data environment (CDE).*<br>• *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*<br>• *System components that could impact the security of account data.* | All data transferred between the hosted data and the operational PCs is encrypted and provided via private web services using TLS 1.2. Access to these web services is limited to the software and must first be authenticated as a valid client and client member. The transfer of data between Azure storage centres (for backup) is managed via dedicated private networks encrypted with a 2048 bit SSL certificate. All data stored within Azure is encrypted at rest with 256 Bit AES Encryption. All client data is stored within unique Microsoft Azure SQL database |
| Indicate whether the environment includes segmentation to reduce the scope of the assessment.<br>*(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)* | ☐ Yes ☒ No |

### Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities (for example, 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 Centre | 1 | london (UK South MIcrosoft Azure) |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## Part 2. Executive Summary *(continued)*

### Part 2e. PCI SSC Validated Products and Solutions

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

☐ Yes ☒ No

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

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

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

## Part 2. Executive Summary *(continued)*

### Part 2f. Third-Party Service Providers

For the services being validated, does the entity have relationships with one or more third-party service providers that:

| | |
|---|---|
| • Store, process, or transmit account data on the entity'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 entity'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 entity'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:** |
|---|---|
| Clone System | PCI Scanning |
| Pay 360 | Payemtn Processing |
| Microsoft Azure | Web and Data Hosting |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

***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 provided within each principal PCI DSS requirement.

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

***Note:*** *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

*Name of Service Assessed:*

| PCI DSS Requirement | Requirement Responses<br>*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 A1: | ☒ | ☐ | ☐ | ☐ | ☐ |
| Appendix A2: | ☐ | ☐ | ☒ | ☐ | ☐ |

**Justification for Approach**

| | |
|---|---|
| For any Not Applicable responses, identify which sub-requirements were not applicable and the reason. | All requirements that are not applicable are because We do not store, process or transmit account data |
| For any Not Tested responses, identify which sub-requirements were not tested and the reason. | |

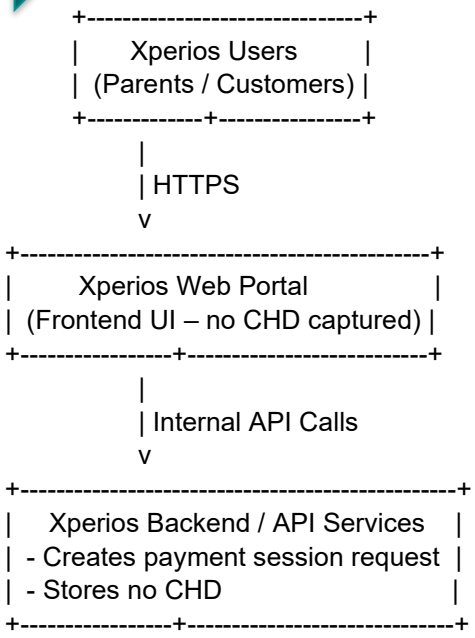
## Section 2a: Details about Reviewed Environment

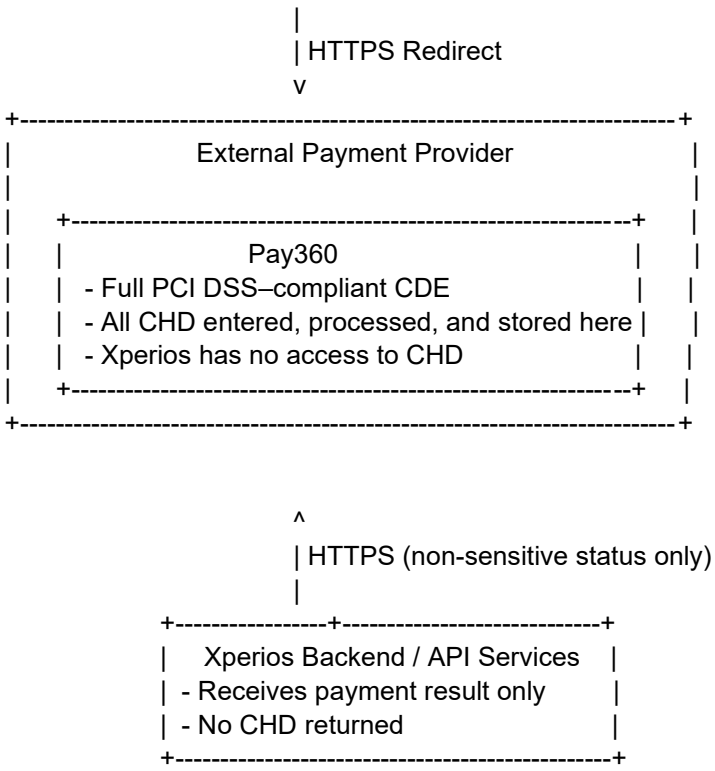
### *Network Diagrams*

Provide one or more network diagrams that:

- Shows all connections between the CDE and other networks, including any wireless networks.
- Is accurate and up to date with any changes to the environment.
- Illustrates all network security controls that are defined for connection points between trusted and untrusted networks.
- Illustrates how system components storing cardholder data are not directly accessible from the untrusted networks.
- Includes the techniques (such as intrusion-detection systems and/or intrusion-prevention systems) that are in place to monitor all traffic:
  - At the perimeter of the cardholder data environment.
  - At critical points in the cardholder data environment.

**<Insert diagram(s) here – one page/image at a time>**






Xperios does not store, process, or transmit cardholder data. No CDE exists within the Xperios environment. All cardholder data is entered and processed exclusively within Pay360's PCI-DSS-compliant environment. The only interaction between Xperios and Pay360 is a secure redirect to initiate payment and a non-sensitive status callback after payment completion

### *Storage of Account Data*

Identify all databases, tables, and files storing account data and provide the following details.

| **Data Store** *Database name, file server name, etc.* | **File name(s), Table names(s) and/or Field names** | **Account data elements stored** *For example, PAN, expiry, name, etc.* | **How data is secured** *For example, what type of encryption and strength, etc.* | **How access to data stores is logged** *Description of logging mechanism used for logging access to data—for example, describe the enterprise log management solution, application-level logging, operating system logging, etc. in place* |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

### *Storage of SAD*

| If SAD is stored complete the following:<br>***Note:*** *Anywhere SAD is stored should be documented in the table above* | |
|---|---|
| Indicate whether SAD is stored post authorization: | ☐ Yes ☐ No |
| Indicate whether SAD is stored as part of Issuer Functions: | ☐ Yes ☐ No |

### *In-Scope System Component Types*

Identify all types of system components in scope.

"System components" include network devices, servers, computing devices, virtual components, cloud components, and software. Examples of system components include but are not limited to:

- Systems that store, process, or transmit account data (for example, payment terminals, authorization systems, clearing systems, payment middleware systems, payment back-office systems, shopping cart and store front systems, payment gateway/switch systems, fraud monitoring systems).
- Systems that provide security services (for example, authentication servers, access control servers, security information and event management (SIEM) systems, physical security systems (for example, badge access or CCTV), multi-factor authentication systems, anti-malware systems).
- Systems that facilitate segmentation (for example, internal network security controls).
- Systems that could impact the security of account data or the CDE (for example, name resolution, or e-commerce (web) redirection servers).
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Cloud infrastructure and components, both external and on premises, and including instantiations of containers or images, virtual private clouds, cloud-based identity and access management, CDEs residing on premises or in the cloud, service meshes with containerized applications, and container orchestration tools.
- Network components, including but not limited to network security controls, switches, routers, CDE network devices, wireless access points, network appliances, and other security appliances.
- Server types, including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- End-user devices, such as computers, laptops, workstations, administrative workstations, tablets, and mobile devices.
- Printers, and multi-function devices that scan, print, and fax.
- Storage of account data in any format (for example, paper, data files, audio files, images, and video recordings).
- Applications, software, and software components, serverless applications, including all purchased, subscribed (for example, Software-as-a-Service), bespoke and custom software, including internal and external (for example, Internet) applications.
- Tools, code repositories, and systems that implement software configuration management or for deployment of objects to the CDE or to systems that can impact the CDE.

For each in-scope system component type, even if it resides within another system component, list below with each component with different roles, vendors, or make/model/version on separate rows. If extra rows are needed, document that separately and consult with the entity to which this SAQ will be submitted about how to provide that information.

| **Type of System Component** *For example, application, firewall, server, IDS, Anti-malware software, database, etc.* | **Total number of system components** *How many system components of this type are in scope* | **Vendor** | **Product Name and Version** | **Role/ Function Description** |
|---|---|---|---|---|
| Web portal | 1 | Paritor Ltd | Xperios | Initiates the redirect to Pay360 |
| Backend Application/API Services | 1 | Microsoft | Azure | generate the payment session request and receive the status callback |
| Web Server / Hosting Environment | 1 | Microsoft | Azure | ensures secure HTTPS and prevents tampering with the redirect |
| Authentication & Session Management | 1 | Microsoft | Azure | ensures only authorised users can initiate payments |
| Configuration Management | 1 | Microsoft | Azure | protects the Pay360 endpoint configuration |
| Logging & Monitoring Systems | 1 | Microsoft | Azure | monitor the payment initiation flow (without logging card data) |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

### *Quarterly Scan Results*

Identify each quarterly ASV scan performed within the last 12 months in the table below. Refer to PCI DSS Requirement 11.3.2 for information about initial PCI DSS assessments against the ASV scan requirements.

| Date of the scan(s) | Name of ASV that performed the scan | Were any vulnerabilities found that resulted in a failed initial scan? | | For all scans resulting in a Fail, provide date(s) of re-scans showing that the vulnerabilities have been corrected |
|---|---|---|---|---|
| | | Yes | No | |
| 04/06/2025 | Serverscan | ☐ | ☒ | |
| 04/06/2025 | Serverscan | ☐ | ☒ | |
| 04/09/2025 | Serverscan | ☐ | ☒ | |
| 04/12/2025 | Serverscan | ☐ | ☒ | |
| Indicate whether this is the assessed entity's initial PCI DSS assessment against the ASV scan requirements. | | | | ☐ Yes ☒ No |
| If **yes**, Identify the name of the document the assessor verified to include the entity's documented policies and procedures requiring scanning at least once every three months going forward. | | | | |
| Assessor comments, if applicable: | | | | |

### *Attestations of Scan Compliance*

The scan must cover all externally accessible (Internet-facing) IP addresses in existence at the entity, in accordance with the *PCI DSS Approved Scanning Vendors (ASV) Program Guide.*

| | |
|---|---|
| Indicate whether the ASV and the assessed entity completed the Attestations of Scan Compliance confirming that all externally accessible (Internet-facing) IP addresses in existence at the entity were appropriately scoped for the ASV scans? | ☒ Yes ☐ No |

# Section 2b: Self-Assessment Questionnaire D for Service Providers

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

**Self-assessment completion date:** 2026/01/26

## 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: | • Examine documentation.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

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

| PCI DSS Requirement | | Expected Testing | Response ♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| | • Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | Our organisation maintains a documented and formal change management process that governs all network connections and any modifications to firewall, routing, or network security configurations. All proposed changes must be submitted through our internal change control workflow, where they undergo review, approval, and risk assessment prior to implementation.<br><br>For systems hosted in Microsoft Azure, network security controls (including Azure Firewall, Network Security Groups, and routing configurations) are managed using role based access control and infrastructure as code deployment pipelines. These pipelines enforce peer review, approval gates, and pre deployment testing in non production environments.<br><br>All changes are logged automatically through Azure Activity Logs and our internal ticketing system, providing a complete audit trail of who made the change, what was changed, and when it occurred. No network change is deployed to production without documented approval and validation.<br><br>This process ensures that all network connections and firewall/router configuration changes are formally reviewed, tested, approved, and recorded in accordance with PCI DSS Requirement 1.1.1. | | | | |
| **1.1.2** | | • Examine documentation. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood. | • Interview responsible personnel. | Our organisation maintains documented roles and responsibilities for all activities required under PCI DSS Requirement 1. These responsibilities include firewall management, network configuration, change control, and ongoing review of network security controls.<br><br>Within Microsoft Azure, these responsibilities are enforced using Azure Role Based Access Control (RBAC), which restricts network related actions to authorised personnel only. Azure Activity Logs provide a complete audit trail of all network changes, ensuring accountability and demonstrating that assigned roles are understood and followed.<br><br>Azure Policy and our Infrastructure as Code deployment pipelines further ensure that only approved individuals can modify network configurations, and that all changes follow our documented processes.<br><br>Azure provides the technical controls to enforce and evidence these responsibilities, while our organisation retains responsibility for defining, documenting, and communicating them in accordance with PCI DSS Requirement 1.1.2 | | | | |

| 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 |
| **1.2** Network security controls (NSCs) are configured and maintained. | | | | | | | |
| **1.2.1** | Configuration standards for NSC rulesets are:<br>• Defined.<br>• Implemented.<br>• Maintained. | • Examine configurations standards.<br>• Examine configuration settings. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation maintains formal configuration standards for all network security controls (NSCs), including Azure Firewall, Network Security Groups (NSGs), routing configurations, and any other components that regulate traffic into or within the cardholder data environment (CDE). These standards define required rule set structures, naming conventions, permitted and denied traffic types, documentation requirements, and review procedures.<br><br>Within Microsoft Azure, these standards are implemented using Azure NSGs, Azure Firewall policies, and infrastructure as code templates that ensure consistent and approved configurations across all environments. Azure Role Based Access Control (RBAC) restricts the ability to modify NSC rule sets to authorised personnel only, and Azure Policy enforces compliance with our defined configuration requirements.<br><br>All NSC rule sets are reviewed regularly and updated as needed to reflect changes in the environment, emerging threats, and organisational requirements. Azure Activity Logs provide a complete audit trail of all configuration changes, ensuring that NSC configurations remain accurate, controlled, and aligned with our documented standards.<br><br>This approach ensures that network security controls are properly configured, consistently maintained, and fully compliant with PCI DSS Requirement 1.2.1. | | | | |

| 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 |
| **1.2.2** | 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.<br>• Examine network configurations.<br>• Examine change control records.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | Changes to network connections include the addition, removal, or modification of a connection.<br>Changes to NSC configurations include those related to the component itself as well as those affecting how it performs its security function. | | Azure provides the technical enforcement, audit logging, and governance capabilities needed to ensure that all changes to network connections and NSC configurations are controlled, approved, and traceable. Our organisation uses these capabilities to meet PCI DSS Requirement 1.2.2 and to ensure that all changes follow our formal change control process. | | | | |
| **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.<br>• Examine network configurations.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement. | Our organisation maintains accurate and up to date network diagrams that document all connections into and out of the cardholder data environment (CDE). Azure provides the technical capabilities and visibility needed to support this requirement.<br><br>Within Microsoft Azure, all virtual networks, subnets, peering connections, private endpoints, VPN/ExpressRoute links, firewalls, and Network Security Groups (NSGs) are centrally defined and visible through the Azure Portal, Azure Resource Graph, and infrastructure as code templates. These tools allow us to identify and document every network path and dependency associated with the CDE.<br><br>Azure's consistent resource structure ensures that any changes to network components—such as new connections, routing updates, or security control modifications—are automatically recorded in Azure Activity Logs. This enables us to keep our diagrams current and aligned with the actual deployed environment.<br><br>Wireless networks, where applicable, are documented separately and shown in relation to the CDE, including segmentation controls that prevent untrusted wireless traffic from accessing CDE resources.<br><br>By using Azure's network visualisation tools, resource inventory, and audit logs, we maintain accurate diagrams that reflect all network connections to the CDE, meeting the intent of PCI DSS Requirement 1.2.3. | | | | |

| 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 |
| **1.2.4** | An accurate data-flow diagram(s) is maintained that meets the following:<br>• Shows all account data flows across systems and networks.<br>• Updated as needed upon changes to the environment. | • Examine data flow diagrams.<br>• Observe network configurations.<br>• Examine documentation.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| | | |
|---|---|---|
| | 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. | Our organisation maintains detailed and current data flow diagrams that document how account data moves across all systems and networks within the cardholder data environment (CDE). Azure provides the technical visibility and resource structure that enable us to accurately identify and map these data flows.<br><br>Within Microsoft Azure, all compute, storage, networking, and integration components are centrally defined and managed. This allows us to clearly identify:<br><br>• Where account data is captured, processed, transmitted, or stored<br><br>• Which Azure services participate in the data flow<br><br>• How data moves between virtual networks, subnets, private endpoints, and application components<br><br>• Any connections to on premises systems or third party services<br><br>Azure Activity Logs, Resource Graph, and infrastructure as code templates provide authoritative information about deployed resources and connectivity. These tools ensure that any changes to the environment—such as new services, updated routing, or modified integrations—are visible and can be reflected promptly in our data flow diagrams.<br><br>Our diagrams are reviewed and updated whenever system changes occur and as part of our regular PCI DSS review cycle. This ensures that they remain accurate and aligned with the actual Azure environment.<br><br>By leveraging Azure's resource inventory, logging, and network visibility capabilities, we maintain accurate and up to date data flow diagrams that meet the intent of PCI DSS Requirement 1.2.4. |

| 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 |
| **1.2.5** | All services, protocols and ports allowed are identified, approved, and have a defined business need. | • Examine documentation.<br>• Examine configuration settings. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation maintains a documented list of approved services, protocols, and ports that are permitted within the cardholder data environment (CDE). Each allowed service or port has a defined business justification, and any non essential or insecure protocols are disabled unless specifically required and protected.<br><br>Microsoft Azure provides the technical controls that support this requirement. Azure Firewall, Network Security Groups (NSGs), and routing configurations allow us to explicitly define and restrict permitted traffic. These controls enforce least privilege access by allowing only approved ports and protocols and blocking all others by default.<br><br>Azure Role Based Access Control (RBAC) ensures that only authorised personnel can modify NSG rules or firewall policies. Azure Activity Logs provide a complete audit trail of all changes to permitted services and ports, enabling us to verify that only approved configurations are implemented.<br><br>Azure Policy further enforces compliance by auditing or preventing the use of unapproved protocols or open ports. This ensures that all allowed services and ports remain aligned with our documented business needs and security standards.<br><br>Through these capabilities, Azure enables us to maintain strict control over permitted services, protocols, and ports, supporting compliance with PCI DSS Requirement 1.2.5. | | | | |

| 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 |
| **1.2.6** | 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.<br>• Examine configuration settings. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation identifies any services, protocols, or ports that are considered insecure and ensures that appropriate security features are defined and implemented to mitigate associated risks. Where such protocols must remain in use, we document the business justification and apply compensating controls.<br><br>Microsoft Azure provides the technical capabilities that support this requirement. Azure Firewall, Network Security Groups (NSGs), and routing controls allow us to tightly restrict the use of insecure protocols and limit their exposure to only approved systems. Azure Policy enables us to detect or prevent the use of unapproved or insecure configurations.<br><br>Azure also provides built in security features—such as TLS enforcement, certificate management, encryption in transit options, and secure protocol defaults—that help mitigate risks when older or less secure protocols must be supported. Azure Activity Logs and RBAC ensure that only authorised personnel can configure these protocols and that all changes are fully auditable.<br><br>Through these controls, Azure enables us to implement and enforce the required security features for any insecure services, protocols, or ports in use, supporting compliance with PCI DSS Requirement 1.2.6. | | | | |

| 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 |
| **1.2.7** | Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective. | • Examine documented procedures.<br>• Examine documentation from reviews performed.<br>• Examine configuration settings. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation performs formal reviews of all network security control (NSC) configurations at least every six months to ensure they remain accurate, relevant, and effective. These reviews include Azure Firewall policies, Network Security Group (NSG) rules, routing configurations, private endpoints, and any other controls governing traffic to and within the cardholder data environment (CDE).<br><br>Microsoft Azure provides the technical capabilities that support this requirement. Azure Activity Logs and Azure Monitor offer complete visibility into configuration changes, enabling us to compare current settings against our approved standards. Azure Resource Graph and infrastructure as code templates allow us to inventory and validate NSC configurations consistently across all environments.<br><br>Azure Policy further assists by identifying deviations from approved configurations, ensuring that any drift is detected and addressed during the review cycle. Azure Role Based Access Control (RBAC) ensures that only authorised personnel can modify NSCs, simplifying the verification of who made changes and when.<br><br>These Azure capabilities enable us to conduct thorough, documented six monthly reviews of all NSC configurations, supporting compliance with PCI DSS Requirement 1.2.7. | | | | |

| 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 |
| **1.2.8** | Configuration files for NSCs are:<br>• Secured from unauthorized access.<br>• Kept consistent with active network configurations. | • Examine NSC configuration files. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | Our organisation ensures that all configuration files for network security controls (NSCs) are protected from unauthorized access and remain consistent with the active configurations deployed in Azure. This includes configuration files, scripts, templates, and infrastructure as code definitions used to manage Azure Firewall, Network Security Groups (NSGs), routing, and other network controls.<br><br>Microsoft Azure provides the technical capabilities that support this requirement. Azure Role Based Access Control (RBAC) restricts access to NSC configuration files and prevents unauthorized users from viewing or modifying them. Azure Storage, Key Vault, and Git based repositories (such as Azure DevOps or GitHub) enforce secure storage, version control, and access auditing for configuration files.<br><br>Azure Activity Logs and Resource Graph allow us to compare deployed NSC configurations with stored configuration files, ensuring consistency and detecting drift. Azure Policy further enforces compliance by identifying or preventing unapproved or inconsistent configurations.<br><br>Through these capabilities, Azure enables us to secure NSC configuration files, maintain alignment between stored and active configurations, and support compliance with PCI DSS Requirement 1.2.8. | | | | |

| 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 |
| **1.3** Network access to and from the cardholder data environment is restricted. | | | | | | | |
| **1.3.1** | Inbound traffic to the CDE is restricted as follows:<br>• To only traffic that is necessary.<br>• All other traffic is specifically denied. | • Examine NSC configuration standards.<br>• Examine NSC configurations. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation restricts inbound traffic to the cardholder data environment (CDE) to only what is required for business operations. All other inbound traffic is explicitly denied. Microsoft Azure provides the technical controls that support this requirement.<br><br>Azure Firewall, Network Security Groups (NSGs), and routing configurations enforce a default deny posture for inbound traffic. Only explicitly defined and approved rules allow traffic into CDE resources. NSGs and firewall policies are configured to permit only the specific ports, protocols, and source networks that have been documented and justified.<br><br>Azure Role Based Access Control (RBAC) ensures that only authorised personnel can modify inbound access rules. Azure Activity Logs provide a complete audit trail of all changes to inbound traffic configurations, enabling verification that only approved rules are implemented.<br><br>Azure Policy further strengthens compliance by detecting or preventing unapproved inbound access configurations, ensuring that the environment maintains a least privilege, deny by default posture.<br><br>Through these capabilities, Azure enables us to tightly control inbound traffic to the CDE and ensure that only necessary, authorised connections are permitted, supporting compliance with PCI DSS Requirement 1.3.1. | | | | |

| 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 |
| **1.3.2** | Outbound traffic from the CDE is restricted as follows:<br>• To only traffic that is necessary.<br>• All other traffic is specifically denied. | • Examine NSC configuration standards.<br>• Examine NSC configurations. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation restricts outbound traffic from the cardholder data environment (CDE) to only what is required for business operations. All other outbound traffic is explicitly denied. Microsoft Azure provides the technical controls that support this requirement.<br><br>Azure Firewall and Network Security Groups (NSGs) enforce a default deny posture for outbound traffic. Only explicitly defined and approved outbound rules are permitted, ensuring that CDE systems can communicate only with authorised destinations, services, and ports. NSGs and firewall policies are configured to allow only the specific outbound traffic that has been documented and justified.<br><br>Azure Role Based Access Control (RBAC) ensures that only authorised personnel can modify outbound access rules. Azure Activity Logs provide a complete audit trail of all changes to outbound traffic configurations, enabling verification that only approved rules are implemented.<br><br>Azure Policy further strengthens compliance by detecting or preventing unapproved outbound access configurations, ensuring that the environment maintains a least privilege, deny by default posture.<br><br>Through these capabilities, Azure enables us to tightly control outbound traffic from the CDE and ensure that only necessary, authorised connections are permitted, supporting compliance with PCI DSS Requirement 1.3.2. | | | | |

| 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 |
| **1.3.3** | NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that:<br>• All wireless traffic from wireless networks into the CDE is denied by default.<br>• Only wireless traffic with an authorized business purpose is allowed into the CDE. | • Examine configuration settings.<br>• Examine network diagrams. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation ensures that all wireless networks are segmented from the cardholder data environment (CDE) using network security controls (NSCs). No wireless network—whether corporate, guest, or operational—has direct access to the CDE. All wireless traffic is denied by default unless a specific, documented business requirement exists.<br><br>Microsoft Azure provides the technical capabilities that support this requirement. Azure virtual networks (VNets) do not include wireless connectivity, and any wireless access occurs outside Azure, typically on premises or through corporate Wi Fi. Connectivity from wireless networks to Azure resources is controlled through Azure Firewall, Network Security Groups (NSGs), VPN gateways, and private endpoints. These controls enforce a strict deny by default posture and allow only explicitly approved traffic paths.<br><br>Azure Role Based Access Control (RBAC) ensures that only authorised personnel can modify segmentation rules. Azure Activity Logs provide a complete audit trail of all changes to NSCs, enabling verification that wireless segmentation remains intact. Azure Policy further assists by detecting or preventing unapproved connectivity configurations.<br><br>Through these capabilities, Azure enables us to enforce strong segmentation between wireless networks and the CDE, ensuring that only authorised wireless traffic is permitted and supporting compliance with PCI DSS Requirement 1.3.3. | | | |

| 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 |
| **1.4** Network connections between trusted and untrusted networks are controlled. | | | | | | | |
| **1.4.1** | NSCs are implemented between trusted and untrusted networks. | • Examine NSC configuration standards.<br>• Examine current network diagrams.<br>• Examine network configurations. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation ensures that all connections between trusted and untrusted networks are controlled using network security controls (NSCs). Microsoft Azure provides the technical capabilities that support this requirement by enforcing segmentation and traffic filtering at every network boundary.<br><br>Azure virtual networks (VNets) are isolated by default, and any connectivity between networks—whether internal, external, or hybrid—must pass through explicitly configured NSCs such as Azure Firewall, Network Security Groups (NSGs), VPN gateways, or private endpoints. These controls enforce a deny by default posture and allow only authorised, business justified traffic to pass between trust zones.<br><br>Azure Role Based Access Control (RBAC) ensures that only authorised personnel can modify NSC configurations. Azure Activity Logs provide a complete audit trail of all changes to network boundaries and security controls. Azure Policy further strengthens compliance by detecting or preventing unapproved configurations that could weaken segmentation.<br><br>Through these capabilities, Azure enables us to implement strong NSCs between trusted and untrusted networks, ensuring that all network boundaries are protected in accordance with PCI DSS Requirement 1.4.1. | | | | |

| 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 |
| **1.4.2** | Inbound traffic from untrusted networks to trusted networks is restricted to:<br>• Communications with system components that are authorized to provide publicly accessible services, protocols, and ports.<br>• Stateful responses to communications initiated by system components in a trusted network.<br>All other traffic is denied. | • Examine NSC documentation.<br>• Examine NSC configurations. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | The intent of this requirement is to address communication sessions between trusted and untrusted networks, rather than the specifics of protocols.<br>This requirement does not limit the use of UDP or other connectionless network protocols if state is maintained by the NSC. | Our organisation ensures that inbound traffic from untrusted networks is tightly controlled and limited to only authorised public facing services. All other inbound traffic is explicitly denied. Microsoft Azure provides the technical capabilities that support this requirement.<br>Azure Firewall and Network Security Groups (NSGs) enforce a deny by default posture for inbound traffic. Only explicitly approved rules allow communication from untrusted networks (such as the internet) to trusted Azure networks. These rules are limited to authorised public facing services, ports, and protocols that have been documented and justified.<br>Azure Firewall is a stateful firewall, meaning it automatically allows return traffic for sessions initiated from trusted networks while blocking unsolicited inbound traffic. This directly supports the requirement to allow only stateful responses to trusted outbound communications.<br>Azure Role Based Access Control (RBAC) ensures that only authorised personnel can modify inbound access rules. Azure Activity Logs provide a complete audit trail of all changes to NSC configurations, enabling verification that only approved inbound paths exist.<br>Azure Policy further strengthens compliance by detecting or preventing unapproved inbound configurations, ensuring that the environment maintains strict segmentation between trusted and untrusted networks.<br>Through these capabilities, Azure enables us to restrict inbound traffic from untrusted networks to only authorised services and stateful responses, supporting compliance with PCI DSS Requirement 1.4.2. | | | | |

| 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 |
| **1.4.3** | Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network. | • Examine NSC documentation.<br>• Examine NSC configurations. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation ensures that anti spoofing protections are in place to prevent forged or manipulated source IP addresses from entering trusted networks. Microsoft Azure provides built in capabilities that support this requirement.<br><br>Azure Firewall includes native anti spoofing protections and stateful packet inspection, automatically blocking traffic with invalid or spoofed source IP addresses. Azure virtual networks (VNets) also enforce system level anti spoofing by preventing virtual machines from sending traffic with IP addresses they are not assigned. Network Security Groups (NSGs) further restrict allowed source IP ranges, ensuring that only authorised and valid sources can reach trusted network segments.<br><br>Azure Role Based Access Control (RBAC) ensures that only authorised personnel can modify these protections. Azure Activity Logs provide a complete audit trail of configuration changes, enabling verification that anti spoofing controls remain active and effective.<br><br>Through these capabilities, Azure enables us to detect and block spoofed traffic at network boundaries, supporting compliance with PCI DSS Requirement 1.4.3. | | | | |
| **1.4.4** | System components that store cardholder data are not directly accessible from untrusted networks. | • Examine the data-flow diagram and network diagram.<br>• Examine NSC configurations. | ☒ | ☐ | ☐ | ☐ | ☐ |

| 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 |
| **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| 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). | | Our organisation ensures that all system components storing cardholder data are isolated from untrusted networks and cannot be accessed directly. Microsoft Azure provides the technical capabilities that support this requirement through strong network segmentation and controlled access paths.<br><br>Azure virtual networks (VNets) are isolated by default, and resources storing cardholder data are placed in private subnets with no public IP addresses. Access to these components is only possible through authorised, controlled pathways such as private endpoints, VPN gateways, or Azure Firewall. Direct inbound access from the internet or any other untrusted network is explicitly denied.<br><br>Azure Firewall and Network Security Groups (NSGs) enforce a deny by default posture, ensuring that only approved traffic from trusted networks can reach CDE systems. Azure Role Based Access Control (RBAC) restricts who can modify these controls, and Azure Activity Logs provide a complete audit trail of all configuration changes.<br><br>Azure Policy further strengthens compliance by detecting or preventing configurations that would expose CDE components to untrusted networks, ensuring that segmentation remains intact.<br><br>Through these capabilities, Azure enables us to ensure that system components storing cardholder data are never directly accessible from untrusted networks, supporting compliance with PCI DSS Requirement 1.4.4. | | | | |

| 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 |
| **1.4.5** | The disclosure of internal IP addresses and routing information is limited to only authorized parties. | • Examine NSC configurations.<br>• Examine documentation.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation ensures that internal IP addressing, routing information, and network topology details are accessible only to authorised personnel. Microsoft Azure provides the technical capabilities that support this requirement.<br><br>Azure virtual networks (VNets), subnets, private endpoints, and routing tables are not publicly exposed. Internal IP addresses are only visible within the Azure environment or through authenticated management interfaces. Azure Role Based Access Control (RBAC) restricts access to network configuration information so that only authorised administrators can view or modify internal addressing and routing.<br><br>Azure Firewall and Network Security Groups (NSGs) prevent accidental exposure of internal IPs by blocking unauthorised inbound and outbound traffic. Azure Private Link further ensures that services are accessed via private IPs without exposing internal addressing to the public internet.<br><br>Azure Activity Logs provide a complete audit trail of access to network configuration data, enabling verification that only authorised parties have viewed or modified internal routing or IP information.<br><br>Through these capabilities, Azure enables us to limit the disclosure of internal IP addresses and routing information to authorised personnel only, supporting compliance with PCI DSS Requirement 1.4.5. | | | | |

| 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 |
| **1.5** 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.<br>• Specific configuration settings are defined to prevent threats being introduced into the entity's network.<br>• Security controls are actively running.<br>• 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.<br>• Examine device configuration settings. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | 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.<br>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. | Our organisation ensures that all computing devices capable of connecting to both untrusted networks and the cardholder data environment (CDE) are secured with centrally managed security controls. Microsoft Azure provides the technical capabilities that support this requirement through strong access pathways, device level enforcement, and management tooling.<br>Access to Azure hosted CDE resources is restricted to managed devices that comply with our security baselines. Azure Active Directory (Azure AD) and Conditional Access enforce that only devices meeting defined configuration requirements—such as active antivirus, disk encryption, secure configuration, and up to date patches—can connect to the CDE. These controls prevent threats from being introduced into the environment.<br>Azure AD Join, Intune, and Endpoint Manager ensure that required security controls are always running and cannot be disabled or altered by end users. Device configuration profiles, compliance policies, and security baselines enforce settings such as firewall enablement, malware protection, OS hardening, and restricted administrative privileges.<br>Azure Activity Logs and Intune audit logs provide full visibility into device compliance and configuration changes, enabling verification that controls remain active and unaltered unless explicitly authorised by management.<br>Through these capabilities, Azure enables us to ensure that only secure, compliant, and centrally managed devices can access the CDE, supporting compliance with PCI DSS Requirement 1.5.1. | | | | |

## *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: | • Examine documentation.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

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

| PCI DSS Requirement | | Expected Testing | Response ♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| | • Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | Our organisation maintains documented and up to date security policies and operational procedures governing the secure configuration of all Azure hosted system components. These procedures define how secure baselines are applied, maintained, and reviewed across Azure resources.<br><br>Microsoft Azure provides the technical capabilities that support this requirement. Azure Policy enforces secure configuration standards across subscriptions and resources, ensuring that documented procedures are consistently applied. Azure Blueprints and infrastructure as code templates (such as ARM or Bicep) allow us to codify secure configurations so they remain repeatable, version controlled, and aligned with our documented policies.<br><br>Azure Role Based Access Control (RBAC) ensures that only authorised personnel can modify configurations, while Azure Activity Logs provide a complete audit trail of changes, enabling verification that procedures are being followed. Azure Advisor and Security Center (Defender for Cloud) provide continuous visibility into configuration compliance, reinforcing adherence to our documented standards.<br><br>Through these capabilities, Azure enables us to maintain, enforce, and operationalise secure configuration policies and procedures, supporting compliance with PCI DSS Requirement 2.1.1. | | | | |
| **2.1.2** | | • Examine documentation. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood. | • Interview responsible personnel. | Our organisation maintains documented roles and responsibilities for all personnel involved in applying and managing secure configurations for Azure hosted system components. These responsibilities are formally assigned and communicated to ensure that all individuals understand their duties.<br><br>Microsoft Azure provides the technical capabilities that support this requirement. Azure Role Based Access Control (RBAC) allows us to assign precise permissions to individuals and teams based on their documented responsibilities. Access is granted according to the principle of least privilege, ensuring that personnel can perform only the configuration tasks aligned with their assigned roles.<br><br>Azure Activity Logs and Azure AD audit logs provide visibility into who performed configuration actions, enabling verification that responsibilities are being followed as documented. Azure Policy and governance tooling reinforce these assignments by ensuring that only authorised roles can modify secure configuration settings.<br><br>Through these capabilities, Azure enables us to clearly define, assign, and enforce roles and responsibilities related to secure configuration management, supporting compliance with PCI DSS Requirement 2.1.2. | | | | |
| **2.2** System components are configured and managed securely. | | | | | | | |
| **2.2.1** | Configuration standards are developed, implemented, and maintained to: | • Examine system configuration standards. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| | | | |
|---|---|---|---|
| | • Cover all system components.<br>• Address all known security vulnerabilities.<br>• Be consistent with industry-accepted system hardening standards or vendor hardening recommendations.<br>• Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1.<br>• 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. | • Review industry-accepted hardening standards.<br>• Examine configuration settings.<br>• Interview personnel. | Our organisation maintains secure configuration standards for all Azure hosted system components. These standards are based on industry accepted hardening guidance and vendor recommendations and are updated as new vulnerabilities are identified. Azure provides the technical capabilities that support the implementation and enforcement of these standards.<br><br>Azure Policy enables us to enforce secure configuration baselines across virtual machines, networks, storage, and platform services. Policies can audit or block non compliant configurations, ensuring that only hardened, approved settings are applied. Azure Blueprints and infrastructure as code templates (ARM/Bicep/Terraform) allow us to deploy systems using pre approved secure configurations, ensuring consistency and compliance before resources enter production.<br><br>Azure Defender for Cloud provides continuous assessment of configuration compliance against industry benchmarks, including CIS and Microsoft security baselines. It identifies deviations, known vulnerabilities, and misconfigurations, enabling timely remediation. Azure Update Management ensures that systems remain patched and aligned with our configuration standards.<br><br>Azure Role Based Access Control (RBAC) restricts who can modify configurations, while Azure Activity Logs provide a complete audit trail of changes, supporting verification that standards are implemented and maintained.<br><br>Through these capabilities, Azure enables us to develop, apply, and maintain secure configuration standards across all system components, supporting compliance with PCI DSS Requirement 2.2.1. |

| 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 |
| **2.2.2** | Vendor default accounts are managed as follows:<br>• If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6.<br>• If the vendor default account(s) will not be used, the account is removed or disabled. | • Examine system configuration standards.<br>• Examine vendor documentation.<br>• Observe a system administrator logging on using vendor default accounts.<br>• Examine configuration files.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | 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.<br>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. | Our organisation ensures that all vendor default accounts associated with Azure hosted systems are either secured or disabled in accordance with our configuration standards. Microsoft Azure provides the technical capabilities that support this requirement.<br>Azure virtual machines and platform services do not expose or require vendor default accounts by default. When deploying operating systems or applications through Azure Marketplace images, we are required to create unique administrative credentials during provisioning, ensuring that no vendor default passwords remain active.<br>Azure Active Directory (Azure AD) and Role Based Access Control (RBAC) provide centralised identity and access management, eliminating the need for local vendor default accounts on most Azure services. Where local accounts exist (for example, on virtual machines), Azure Policy, Azure Automation, and configuration management tools (such as Intune, Desired State Configuration, or third party CM tools) enforce the removal or disabling of unused default accounts and ensure that any required accounts have secure, non default credentials.<br>Azure Activity Logs and Azure AD audit logs provide full visibility into account creation, modification, and authentication activity, enabling verification that vendor default accounts are not present or are properly secured.<br>Through these capabilities, Azure enables us to ensure that vendor default accounts are either disabled or secured with unique credentials, supporting compliance with PCI DSS Requirement 2.2.2. | | | | |

| 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 |
| **2.2.3** | Primary functions requiring different security levels are managed as follows:<br>• Only one primary function exists on a system component,<br>**OR**<br>• Primary functions with differing security levels that exist on the same system component are isolated from each other,<br>**OR**<br>• 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. | • Examine system configuration standards.<br>• Examine system configurations. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation ensures that system components in Azure are designed so that primary functions with differing security requirements are either separated, isolated, or uniformly hardened to the highest required level. Microsoft Azure provides the technical capabilities that support this requirement.<br><br>Azure virtual networks (VNets), subnets, and network security controls allow us to separate system functions onto distinct components when required. Where multiple functions exist on the same system component—such as a virtual machine—Azure enables strong isolation through OS level hardening, role separation, and application sandboxing. Infrastructure as code templates and Azure Policy ensure that all deployed components follow our secure configuration standards, including cases where functions must be secured to the highest applicable security level.<br><br>Azure Role Based Access Control (RBAC) restricts administrative access to each function according to its security classification. Azure Activity Logs provide a complete audit trail of configuration changes, enabling verification that isolation or hardening controls remain in place.<br><br>Through these capabilities, Azure enables us to separate, isolate, or uniformly secure system functions according to their required security levels, supporting compliance with PCI DSS Requirement 2.2.3. | | | | |

| 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 |
| **2.2.4** | | | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled. | • Examine system configuration standards.<br>• Examine system configurations. | Our organisation ensures that only required services and functions are enabled on Azure hosted system components, and all unnecessary services, protocols, and daemons are disabled in accordance with our secure configuration standards. Microsoft Azure provides the technical capabilities that support this requirement.<br><br>Azure virtual machines and platform services can be deployed using hardened images that include only approved services. Azure Policy enforces configuration rules that prevent the use of insecure or unnecessary protocols (such as legacy TLS versions, SMBv1, or open management ports). Infrastructure as code templates ensure that deployed systems include only the services defined in our configuration standards.<br><br>Azure Defender for Cloud continuously assesses system components for unnecessary or insecure services and provides recommendations to disable them. Update Management and configuration management tools (such as Intune, Desired State Configuration, or third party CM solutions) enforce ongoing compliance by ensuring that only authorised services remain active.<br><br>Azure Role Based Access Control (RBAC) restricts who can enable or modify system services, while Azure Activity Logs provide a complete audit trail of configuration changes, enabling verification that unnecessary functionality is not enabled.<br><br>Through these capabilities, Azure enables us to ensure that only necessary services and protocols are active on system components, supporting compliance with PCI DSS Requirement 2.2.4. | | | | |

| 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 |
| **2.2.5** | If any insecure services, protocols, or daemons are present: | • Examine configuration standards. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| • Business justification is documented.<br>• Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons. | • Interview personnel.<br>• Examine configuration settings. | Our organisation ensures that any insecure services or protocols used within Azure environments are formally documented, justified, and protected with compensating security controls. Microsoft Azure provides the technical capabilities that support this requirement.<br><br>Azure Policy allows us to detect and prevent the use of insecure protocols such as legacy TLS versions, outdated cipher suites, or deprecated management ports. When a business requirement necessitates the use of an insecure protocol, Azure Defender for Cloud provides continuous monitoring and alerts, ensuring that compensating controls—such as network segmentation, encryption, or restricted access—are implemented.<br><br>Azure Firewall and Network Security Groups (NSGs) restrict access to insecure services to only authorised systems and networks. Azure Private Link and VPN gateways ensure that traffic using such protocols is isolated from untrusted networks. Configuration management tools (such as Desired State Configuration, Intune, or third party CM solutions) enforce secure settings and ensure that additional controls remain active.<br><br>Azure Activity Logs and Azure AD audit logs provide a complete audit trail of configuration changes and access, enabling verification that insecure protocols are used only when justified and with appropriate risk reducing controls.<br><br>Through these capabilities, Azure enables us to document, justify, and secure any required insecure services or protocols, supporting compliance with PCI DSS Requirement 2.2.5. | | | | |

| 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 |
| **2.2.6** | System security parameters are configured to prevent misuse. | • Examine system configuration standards. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| | | | |
|---|---|---|---|
| | | • Interview personnel.<br>• Examine system configurations. | Our organisation configures all Azure hosted system components with security parameters designed to prevent misuse, unauthorised access, and insecure behaviour. Microsoft Azure provides the technical capabilities that support this requirement.<br><br>Azure Policy enforces secure configuration settings across virtual machines, networks, storage, and platform services. Policies ensure that required security parameters—such as password complexity, encryption, logging, secure protocols, and restricted management access—are consistently applied and cannot be bypassed.<br><br>Azure Defender for Cloud continuously evaluates system configurations against industry benchmarks and identifies weak or misconfigured security parameters. Recommendations help ensure that parameters remain aligned with our secure configuration standards.<br><br>Azure Role Based Access Control (RBAC) restricts who can modify system security parameters, preventing unauthorised changes. Azure Activity Logs and Azure AD audit logs provide a complete record of configuration modifications, enabling verification that security parameters remain in place and are not altered improperly.<br><br>Configuration management tools (such as Desired State Configuration, Intune, or third party CM solutions) enforce approved settings and automatically remediate deviations, ensuring that system parameters remain hardened against misuse.<br><br>Through these capabilities, Azure enables us to configure, enforce, and maintain system security parameters that prevent misuse, supporting compliance with PCI DSS Requirement 2.2.6. |

| 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 |
| **2.2.7** | All non-console administrative access is encrypted using strong cryptography. | • Examine system configuration standards.<br>• Observe an administrator log on.<br>• Examine system configurations.<br>• Examine vendor documentation.<br>Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | This includes administrative access via browser-based interfaces and application programming interfaces (APIs). | Our organisation ensures that all administrative access to Azure hosted system components is encrypted using strong cryptography. Microsoft Azure provides the technical capabilities that support this requirement.<br><br>Azure requires secure, encrypted protocols for all remote administrative access. Administrative connections to virtual machines use SSH with strong ciphers for Linux and RDP over TLS for Windows. Azure Bastion provides an additional hardened, TLS encrypted access layer that eliminates the need to expose management ports to the internet. Administrative access to Azure services and management interfaces—such as the Azure Portal, Azure CLI, Azure PowerShell, and REST APIs—is always encrypted using HTTPS with strong TLS configurations.<br><br>Azure Policy enforces the use of secure protocols and can block or audit insecure configurations. Azure Defender for Cloud continuously monitors for weak encryption, deprecated protocols, or exposed management ports, providing alerts and remediation guidance.<br><br>Azure Role Based Access Control (RBAC) ensures that only authorised personnel can perform administrative actions, while Azure Activity Logs provide a complete audit trail of administrative access and configuration changes.<br><br>Through these capabilities, Azure ensures that all non console administrative access is encrypted using strong cryptography, supporting compliance with PCI DSS Requirement 2.2.7. | | | | |

| 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 |
| **2.3** 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:<br>• Default wireless encryption keys.<br>• Passwords on wireless access points.<br>• SNMP defaults.<br>Any other security-related wireless vendor defaults. | • Examine policies and procedures.<br>• Review vendor documentation.<br>• Examine wireless configuration settings.<br>Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | 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. | | Our organisation ensures that no wireless technologies are deployed within the Azure hosted cardholder data environment (CDE). Azure does not provide or rely on wireless networking for access to virtual networks or system components, eliminating the risk of wireless vendor defaults within the cloud environment.<br><br>Where wireless access is used by administrators or staff to reach Azure resources (for example, from corporate devices), Azure Active Directory (Azure AD) and Conditional Access enforce strong authentication, device compliance, and encrypted connections. These controls ensure that only secure, managed devices can access the CDE, regardless of the wireless network they use.<br><br>Azure services are accessed exclusively through encrypted channels such as HTTPS/TLS, VPN, or ExpressRoute. No Azure service exposes or relies on wireless access points, wireless encryption keys, SNMP defaults, or other wireless vendor settings.<br><br>Through these capabilities, Azure ensures that wireless vendor defaults do not exist within the cloud environment and that any wireless access to Azure resources is secured through strong authentication and encryption, supporting compliance with PCI DSS Requirement 2.3.1. | | | | |
| **2.3.2** | | • Examine key-management documentation. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows:<br>• Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary.<br>• Whenever a key is suspected of or known to be compromised. | • Interview personnel. | Our organisation does not use wireless technologies within the Azure hosted cardholder data environment (CDE). Azure virtual networks, private endpoints, and management interfaces do not rely on wireless encryption keys, wireless access points, or shared wireless credentials. As a result, no wireless keys exist within the Azure environment that would require rotation or compromise management.<br><br>Where administrators access Azure resources from corporate wireless networks, Azure Active Directory (Azure AD) and Conditional Access enforce strong authentication, device compliance, and encrypted connections. Access to Azure services occurs exclusively over secure channels such as HTTPS/TLS, VPN, or ExpressRoute, none of which rely on shared wireless keys.<br><br>Wireless key rotation policies are applied within our on premises or corporate wireless infrastructure, independent of Azure. Azure's identity based access model ensures that even if a wireless key were compromised, access to Azure resources would still require strong authentication and authorisation.<br><br>Through these capabilities, Azure ensures that wireless encryption keys are not used within the cloud environment and that any wireless access to Azure resources is protected by strong identity and encryption controls, supporting compliance with PCI DSS Requirement 2.3.2. | | | | |

# 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:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | • Examine documentation.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **3.1.2** | Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood. | • Examine documentation.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |

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

| PCI DSS Requirement | | Expected Testing | Response♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| **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:<br>• Coverage for all locations of stored account data.<br>• Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.*<br>• Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements.<br>• Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.<br>• Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.<br>• 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. | • Examine the data retention and disposal policies, procedures, and processes.<br>• Interview personnel.<br>• Examine files and system records on system components where account data is stored.<br>• Observe the mechanisms used to render account data unrecoverable. | ☒ | ☐ | ☐ | ☐ | ☐ |

| 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 |
| | **Applicability Notes** *(continued)* | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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.<br>*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.* | | We do not store, process or transmit account data | | | | |
| **3.3** Sensitive authentication data (SAD) is not stored after authorization. | | | | | | | |
| **3.3.1** | SAD is not stored after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process. | • Examine documented policies and procedures.<br>• Examine system configurations.<br>• Observe the secure data deletion processes. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | Issuers and companies that support issuing services, where there is a legitimate and documented business need to store SAD, are not required to meet this requirement. A legitimate business need is one that is necessary for the performance of the function being provided by or for the issuer.<br>Refer to Requirement 3.3.3 for additional requirements specifically for these entities.<br>Sensitive authentication data includes the data cited in Requirements 3.3.1.1 through 3.3.1.3. | | We do not store, process or transmit 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 |
| **3.3.1.1** | The full contents of any track are not stored upon completion of the authorization process. | • Examine data sources. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | In the normal course of business, the following data elements from the track may need to be retained:<br>• Cardholder name.<br>• Primary account number (PAN).<br>• Expiration date.<br>• Service code.<br>To minimize risk, store securely only these data elements as needed for business. | | We do not store, process or transmit account data | | | | |
| **3.3.1.2** | The card verification code is not stored upon completion of the authorization process. | • Examine data sources. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | We do not store, process or transmit account data | | | | |
| **3.3.1.3** | The personal identification number (PIN) and the PIN block are not stored upon completion of the authorization process. | • Examine data sources. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | We do not store, process or transmit 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 |
| **3.3.2** | SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography. | • Examine data stores and system configurations.<br>• Examine vendor documentation. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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 these organizations for any additional criteria.<br>This requirement applies to all storage of SAD, even if no PAN is present in the environment.<br>Refer to Requirement 3.2.1 for an additional requirement that applies if SAD is stored prior to completion of authorization.<br>Issuers and companies that support issuing services, where there is a legitimate and documented business need to store SAD, are not required to meet this requirement. A legitimate business need is one that is necessary for the performance of the function being provided by or for the issuer.<br>Refer to Requirement 3.3.3 for requirements specifically for these entities.<br>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.<br>*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.* | | We do not store, process or transmit 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 |
| 3.3.3 | ***Additional requirement for issuers and companies that support issuing services and store sensitive authentication data***:<br>Any storage of sensitive authentication data is:<br>• Limited to that which is needed for a legitimate issuing business need and is secured.<br>• Encrypted using strong cryptography. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* | • Examine documented policies.<br>• Interview personnel.<br>• Examine data stores and system configurations. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only to issuers and companies that support issuing services and store sensitive authentication data.<br>Entities that issue payment cards or that perform or support issuing services will often create and control sensitive authentication data as part of the issuing function. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF they have a legitimate business need to store such data.<br>A legitimate issuing business need is one that is necessary for the performance of the function being provided by or for the issuer.<br>*The bullet above (for encrypting stored SAD with strong cryptography) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.3.3 and must be fully considered during a PCI DSS assessment.* | | We do not store, process or transmit 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 |
| **3.4** Access to displays of full PAN and ability to copy PAN are restricted. | | | | | | | |
| **3.4.1** | PAN is masked when displayed (the BIN and last four digits **are the maximum number** of digits to be displayed), such that only personnel with a legitimate business need can see **more than** the BIN and last four digits of the PAN. | • Examine documented policies and procedures.<br>• Examine system configurations.<br>• Examine the documented list of roles that need access to more than the BIN and last four digits of the PAN (includes full PAN).<br>• Examine displays of PAN (for example, on screen, on paper receipts). | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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.<br>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. | | We do not store, process or transmit 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 |
| **3.4.2** | 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. | • Examine documented policies and procedures and documented evidence for technical controls.<br>• Examine configurations for remote-access technologies.<br>• Observe processes.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS.<br>*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.* | | We do not store, process or transmit 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 |
| **3.5** 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:<br>• One-way hashes based on strong cryptography of the entire PAN.<br>• Truncation (hashing cannot be used to replace the truncated segment of PAN).<br>– 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<br>• Index tokens.<br>• Strong cryptography with associated key-management processes and procedures. | • Examine documentation about the system used to render PAN unreadable.<br>• Examine data repositories.<br>• Examine audit logs, including payment application logs.<br>• Examine controls to verify that the hashed and truncated PANs cannot be correlated to reconstruct the original PAN. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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).<br>This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN. | | We do not store, process or transmit account data | | | | |
| **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 key-management processes and procedures in accordance with Requirements 3.6 and 3.7. | • Examine documentation about the hashing method used.<br>• Examine documentation about the key-management procedures and processes.<br>• Examine data repositories.<br>• Examine audit logs, including payment application logs. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | All Applicability Notes for Requirement 3.5.1 also apply to this requirement.<br>Key-management processes and procedures (Requirements 3.6 and 3.7) do not apply to system components used to generate individual keyed hashes of a PAN for comparison to another system if:<br>• The system components only have access to one hash value at a time (hash values are not stored on the system)<br>**AND**<br>• There is no other account data stored on the same system as the hashes.<br>*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. This requirement will replace the bullet in Requirement 3.5.1 for one-way hashes once its effective date is reached.* | | We do not store, process or transmit 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 |
| **3.5.1.2** | If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows:<br>• On removable electronic media.<br>**OR**<br>• If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1. | • Observe encryption processes.<br>• Examine configurations and/or vendor documentation.<br>• Observe encryption processes. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies to any encryption method that provides clear-text PAN automatically when a system runs, even though an authorized user has not specifically requested that data.<br>While disk or partition 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 data-level 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.<br>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.<br>Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.<br>For issuers and companies that support issuing services: This requirement does not apply to PANs being accessed for real-time transaction processing. However, it does apply to PANs stored for other purposes.<br>*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.* | | We do not store, process or transmit 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 |
| **3.5.1.3** | 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:<br>• Logical access is managed separately and independently of native operating system authentication and access control mechanisms.<br>• Decryption keys are not associated with user accounts.<br>• Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely. | • Examine system configurations.<br>• Observe the authentication process.<br>• Examine files containing authentication factors.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements. | | We do not store, process or transmit 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 |
| **3.6** 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:<br>• Access to keys is restricted to the fewest number of custodians necessary.<br>• Key-encrypting keys are at least as strong as the data-encrypting keys they protect.<br>• Key-encrypting keys are stored separately from data-encrypting keys.<br>• Keys are stored securely in the fewest possible locations and forms. | • Examine documented key-management policies and procedures. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies to keys used to protect stored account data and to key-encrypting keys used to protect data-encrypting keys.<br>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 key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures. | | We do not store, process or transmit 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 |
| 3.6.1.1 | ***Additional requirement for service providers only:***<br>A documented description of the cryptographic architecture is maintained that includes:<br>• Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date.<br>• Preventing the use of the same cryptographic keys in production and test environments. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.*<br>• Description of the key usage for each key.<br>• Inventory of any hardware security modules (HSMs), key-management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, to support meeting Requirement 12.3.4. | • Examine cryptographic architecture documentation.<br>• Interview responsible personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a service provider.<br>In cloud HSM implementations, responsibility for the cryptographic architecture according to this Requirement will be shared between the cloud provider and the cloud customer.<br>*The bullet above (for including, in the cryptographic architecture, that the use of the same cryptographic keys in production and test is prevented) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.6.1.1 and must be fully considered during a PCI DSS assessment.* | | We do not store, process or transmit 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 |
| **3.6.1.2** | Secret and private keys used to protect stored account data are stored in one (or more) of the following forms at all times:<br>• 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.<br>• Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device.<br>• As at least two full-length key components or key shares, in accordance with an industry-accepted method. | • Examine documented procedures.<br>• Examine system configurations and key storage locations, including for key-encrypting keys. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | It is not required that public keys be stored in one of these forms.<br>Cryptographic keys stored as part of a key-management system (KMS) that employs SCDs are acceptable.<br>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:<br>• Using an approved random number generator and within an SCD,<br>**OR**<br>• According to ISO 19592 or equivalent industry standard for generation of secret key shares. | | We do not store, process or transmit account data | | | | |
| **3.6.1.3** | Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary. | • Examine user access lists. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **3.6.1.4** | Cryptographic keys are stored in the fewest possible locations. | • Examine key storage locations.<br>• Observe processes. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **3.7** 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.<br>• Observe the method for generating keys. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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.<br>• Observe the method for distributing keys. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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.<br>• Observe the method for storing keys. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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:<br>• A defined cryptoperiod for each key type in use.<br>• A process for key changes at the end of the defined cryptoperiod. | • Examine documented key-management policies and procedures.<br>• Interview personnel.<br>• Observe key storage locations. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **3.7.5** | 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:<br>• The key has reached the end of its defined cryptoperiod.<br>• 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.<br>• The key is suspected of or known to be compromised.<br>Retired or replaced keys are not used for encryption operations. | • Examine documented key-management policies and procedures.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). | | We do not store, process or transmit 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 |
| **3.7.6** | Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented including managing these operations using split knowledge and dual control. | • Examine documented key-management policies and procedures.<br>• Interview personnel.<br>• Observe processes. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This control is applicable for manual key-management operations.<br>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:<br>• Using an approved random number generator and within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device,<br>**OR**<br>• According to ISO 19592 or equivalent industry standard for generation of secret key shares. | | We do not store, process or transmit account data | | | | |
| **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.<br>• Interview personnel.<br>• Observe processes. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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 key-custodian responsibilities. | • Examine documented key-management policies and procedures.<br>• Review documentation or other evidence of key custodian acknowledgments. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **3.7.9** | ***Additional requirement for service providers only:***<br>Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers. | • Examine documentation provided by the service provider to its customers. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a service provider. | | We do not store, process or transmit account data | | | | |

## *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 understood. | | | | | | | |
| **4.1.1** | All security policies and operational procedures that are identified in Requirement 4 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | • Examine documentation.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **4.1.2** | Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood. | • Examine documentation.<br>• Interview responsible personnel | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |

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

| PCI DSS Requirement | | Expected Testing | Response ♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| **4.2** PAN is protected with strong cryptography during transmission. | | | | | | | |
| **4.2.1** | Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: | | | | | | |
| | • Only trusted keys and certificates are accepted. | • Examine documented policies and procedures.<br>• Interview personnel.<br>• Examine system configurations.<br>• Examine cardholder data transmissions.<br>• 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** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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..<br>*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.* | | We do not store, process or transmit account data | | | | |
| **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.<br>• Examine the inventory of trusted keys and certificates. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | *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.* | | We do not store, process or transmit account data | | | | |
| **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. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **4.2.2** | PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies. | • Examine documented policies and procedures.<br>• Examine system configurations and vendor documentation. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement also applies if a customer, or other third-party, requests that PAN is sent to them via end-user messaging technologies.<br>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. | | We do not store, process or transmit account data | | | | |

# Maintain a Vulnerability Management Program

## *Requirement 5: Protect All Systems and Networks from Malicious Software*

| PCI DSS Requirement | | Expected Testing | Response ♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not 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: | • Examine documentation.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

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

| PCI DSS Requirement | | Expected Testing | Response ♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| | • Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | Our organisation maintains documented and up to date security policies and operational procedures governing malware protection for all Azure hosted systems. These procedures define how anti malware tools are deployed, monitored, updated, and reviewed across our Azure environment. Policies are communicated to all relevant personnel and are incorporated into our operational processes.<br><br>Microsoft Azure provides the technical capabilities that support this requirement. Azure Defender for Cloud offers continuous assessment of malware protection status, ensuring that anti malware solutions are deployed and functioning on applicable virtual machines and workloads. Azure Policy enforces compliance with our documented standards by auditing or preventing deployments that do not meet our malware protection requirements.<br><br>Azure Activity Logs, Azure Monitor, and Defender for Cloud alerts provide visibility into malware related events and configuration changes, enabling verification that documented procedures are being followed. These tools also support regular reviews and updates to our policies based on emerging threats and operational findings.<br><br>Through these capabilities, Azure enables us to maintain, enforce, and operationalise documented malware protection policies and procedures, supporting compliance with PCI DSS Requirement 5.1.1. | | | | |
| **5.1.2** | | • Examine documentation.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood. | | Our organisation maintains documented roles and responsibilities for all personnel involved in protecting Azure hosted systems from malware. These responsibilities cover deployment, monitoring, updating, and reviewing anti malware controls, and are communicated to ensure all individuals understand their duties.<br><br>Microsoft Azure provides the technical capabilities that support this requirement. Azure Role Based Access Control (RBAC) allows us to assign precise permissions aligned with each documented responsibility, ensuring that only authorised personnel can configure or manage malware protection settings. Azure Defender for Cloud reinforces these assignments by identifying systems lacking required protection and by ensuring that only authorised roles can modify security configurations.<br><br>Azure Activity Logs and Azure AD audit logs provide full visibility into actions taken on system components, enabling verification that responsibilities are being followed as documented. These logs also support periodic reviews to confirm that assigned roles remain appropriate and effective.<br><br>Through these capabilities, Azure enables us to clearly define, assign, and enforce roles and responsibilities related to malware protection, supporting compliance with PCI DSS Requirement 5.1.2. | | | | |
| **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 | • Examine system components. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | 5.2.3 that concludes the system components are not at risk from malware. | • Examine the periodic evaluations. | Our organisation deploys anti malware protection on all Azure hosted system components that are susceptible to malware. Microsoft Azure provides the technical capabilities that support this requirement. Azure Defender for Cloud includes integrated anti malware and endpoint protection recommendations, ensuring that virtual machines and supported workloads have Microsoft Defender for Endpoint or another approved anti malware solution installed, active, and up to date.<br><br>Azure Policy enforces our malware protection standards by auditing or preventing the deployment of virtual machines that do not meet required anti malware configurations. Azure Arc extends this enforcement to hybrid and multi cloud systems where applicable. For system components that are not at risk from malware—such as certain PaaS services or immutable workloads—periodic evaluations are performed in accordance with Requirement 5.2.3, and Azure's service architecture provides built in protections that reduce malware exposure.<br><br>Azure Monitor and Defender for Cloud provide continuous visibility into anti malware status, signature updates, and alerts, enabling us to verify that protection is deployed and functioning as required.<br><br>Through these capabilities, Azure enables us to deploy, enforce, and monitor anti malware protection across all applicable system components, supporting compliance with PCI DSS Requirement 5.2.1. | | | | |
| **5.2.2** | The deployed anti-malware solution(s):<br>• Detects all known types of malware. | • Examine vendor documentation.<br>• Examine system configurations. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| • Removes, blocks, or contains all known types of malware. | | Our organisation deploys anti malware solutions on Azure hosted systems that are capable of detecting, blocking, removing, or containing all known types of malware. Microsoft Azure provides the technical capabilities that support this requirement. Azure Defender for Cloud integrates with Microsoft Defender for Endpoint and other approved anti malware tools, ensuring that deployed solutions use industry recognised threat intelligence feeds, behavioural analysis, and signature based detection to identify known malware.<br><br>Azure Policy enforces the use of approved anti malware agents and prevents or audits deployments that do not meet our malware protection standards. Defender for Cloud continuously monitors the health and configuration of anti malware agents, verifying that real time protection, automatic remediation, and threat response capabilities are active.<br><br>Azure Monitor and Defender for Cloud alerts provide visibility into malware detections and containment actions, enabling verification that the deployed solutions are functioning effectively and responding to threats as required.<br><br>Through these capabilities, Azure enables us to deploy and maintain anti malware solutions that detect, block, remove, or contain known malware, supporting compliance with PCI DSS Requirement 5.2.2. | | | | |

| 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 |
| **5.2.3** | Any system components that are not at risk for malware are evaluated periodically to include the following:<br>• A documented list of all system components not at risk for malware.<br>• Identification and evaluation of evolving malware threats for those system components.<br>• Confirmation whether such system components continue to not require anti-malware protection. | • Examine documented policies and procedures.<br>• Interview personnel.<br>• Examine the list of system components not at risk for malware and compare against the system components without an anti-malware solution deployed. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | System components covered by this requirement are those for which there is no anti-malware solution deployed per Requirement 5.2.1. | | We do not store, process or transmit account data | | | | |
| **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.<br>• Examine documented results of periodic evaluations.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | We do not store, process or transmit account data | | | | |
| **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. | | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | | • Examine anti-malware solution(s) configurations, including any master installation.<br>• Examine system components and logs. | Our organisation ensures that all anti malware solutions deployed on Azure hosted systems are configured to receive automatic updates. Microsoft Azure provides the technical capabilities that support this requirement. Azure Defender for Cloud integrates with Microsoft Defender for Endpoint and other approved anti malware tools, ensuring that real time protection, signature updates, and engine updates are automatically applied.<br><br>Azure Policy enforces the use of anti malware configurations that require automatic updates, preventing or auditing deployments that do not meet this standard. Azure Update Management and Microsoft Defender for Endpoint ensure that anti malware agents remain current across virtual machines and hybrid workloads.<br><br>Azure Monitor, Defender for Cloud alerts, and system logs provide visibility into update status, enabling verification that anti malware solutions are receiving and applying updates as required.<br><br>Through these capabilities, Azure enables us to maintain automatically updated anti malware protection across all applicable system components, supporting compliance with PCI DSS Requirement 5.3.1. | | | | |

| 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 |
| **5.3.2** | The anti-malware solution(s):<br>• Performs periodic scans and active or real-time scans<br>OR<br>• Performs continuous behavioral analysis of systems or processes. | • Examine anti-malware solution(s) configurations, including any master installation.<br>• Examine system components.<br>• Examine logs and scan results. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation deploys anti malware solutions on Azure hosted systems that support real time protection, periodic scanning, and continuous behavioural analysis. Microsoft Azure provides the technical capabilities that support this requirement. Azure Defender for Cloud integrates with Microsoft Defender for Endpoint and other approved anti malware tools, ensuring that deployed agents perform real time monitoring, scheduled scans, and behavioural threat detection.<br><br>Azure Policy enforces the use of approved anti malware configurations, ensuring that workloads are deployed with agents capable of active scanning and behavioural analysis. Defender for Cloud continuously monitors the health and configuration of these agents, verifying that real time protection and periodic scans are enabled and functioning.<br><br>Azure Monitor, Defender for Cloud alerts, and anti malware logs provide visibility into scan results, detections, and behavioural analysis events, enabling verification that the anti malware solution is operating as required.<br><br>Through these capabilities, Azure enables us to deploy and maintain anti malware solutions that provide real time scanning, periodic scanning, and behavioural analysis, supporting compliance with PCI DSS Requirement 5.3.2. | | | | |

| 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 |
| **5.3.2.1** | 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.<br>• Examine documented results of periodic malware scans.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies to entities conducting periodic malware scans to meet Requirement 5.3.2.<br>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. | | We do not store, process or transmit account data | | | | |
| **5.3.3** | For removable electronic media, the anti-malware solution(s):<br>• Performs automatic scans of when the media is inserted, connected, or logically mounted,<br>**OR**<br>• Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted. | • Examine anti-malware solution(s) configurations.<br>• Examine system components with removable electronic media.<br>• Examine logs and scan results. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | We do not store, process or transmit 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 |
| **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. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation ensures that audit logs for all anti malware solutions deployed on Azure hosted systems are enabled and retained in alignment with our PCI DSS logging and retention policies. Microsoft Azure provides the technical capabilities that support this requirement. Anti malware agents integrated through Azure Defender for Cloud and Microsoft Defender for Endpoint generate detailed security and operational logs, including malware detections, remediation actions, scan results, and agent health.<br><br>Azure Monitor and Log Analytics collect and centralise these logs, enabling long term retention consistent with Requirement 10.5.1. Azure Policy enforces logging configurations to ensure anti malware agents cannot be deployed without audit logging enabled. Defender for Cloud continuously monitors log ingestion and alerts on missing or misconfigured logging.<br><br>Through these capabilities, Azure enables us to ensure that anti malware audit logs are generated, captured, and retained in accordance with PCI DSS requirements, supporting compliance with Requirement 5.3.4. | | | | |
| **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.<br>• Observe processes.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | Anti-malware solutions may be temporarily disabled only if there is a legitimate technical need, as authorized by management on a case-by-case basis. If anti-malware protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which anti-malware protection is not active. | | Our organisation ensures that users cannot disable or modify anti malware mechanisms on Azure hosted systems without explicit, documented, and time limited management approval. Microsoft Azure provides the technical capabilities that support this requirement. Azure Role Based Access Control (RBAC) restricts administrative permissions so that only authorised personnel can modify anti malware configurations. Standard users and application identities do not have the privileges required to disable or alter anti malware agents.<br><br>Azure Defender for Cloud continuously monitors anti malware status and alerts if protection is disabled, tampered with, or misconfigured. Azure Policy enforces configuration baselines that prevent workloads from being deployed or operated without required anti malware settings. Any approved temporary exceptions are documented internally and monitored through Azure Activity Logs, which provide a full audit trail of configuration changes.<br><br>Through these capabilities, Azure enables us to prevent unauthorised modification of anti malware mechanisms and to tightly control and monitor any approved, time limited exceptions, supporting compliance with PCI DSS Requirement 5.3.5. | | | | |
| **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.<br>• Examine mechanisms. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | The focus of this requirement is on protecting personnel with access to system components in-scope for PCI DSS.<br>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.<br>*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.* | Our organisation ensures that users cannot disable or modify anti malware mechanisms on Azure hosted systems without explicit, documented, and time limited management approval. Microsoft Azure provides the technical capabilities that support this requirement. Azure Role Based Access Control (RBAC) restricts administrative permissions so that only authorised personnel can modify anti malware configurations. Standard users and application identities do not have the privileges required to disable or alter anti malware agents.<br>Azure Defender for Cloud continuously monitors anti malware status and alerts if protection is disabled, tampered with, or misconfigured. Azure Policy enforces configuration baselines that prevent workloads from being deployed or operated without required anti malware settings. Any approved temporary exceptions are documented internally and monitored through Azure Activity Logs, which provide a full audit trail of configuration changes.<br>Through these capabilities, Azure enables us to prevent unauthorised modification of anti malware mechanisms and to tightly control and monitor any approved, time limited exceptions, supporting compliance with PCI DSS Requirement 5.3.5. | | | | |

## *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:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>Known to all affected parties. | • Examine documentation.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation maintains documented, up to date security policies and operational procedures for all activities defined in Requirement 6. These procedures are communicated to all relevant personnel and embedded into our secure development and secure maintenance processes. Microsoft Azure provides the governance and technical capabilities that support this requirement. Azure Policy, Defender for Cloud, and DevOps tooling ensure that documented procedures are enforced and remain current. Azure AD role assignments, audit logs, and security dashboards provide visibility that policies are in use and understood by affected parties. Through these capabilities, Azure enables us to maintain, enforce, and evidence the policies and procedures required by PCI DSS Requirement 6.1.1. | | | | |
| **6.1.2** | | • Examine documentation. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

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

| PCI DSS Requirement | | Expected Testing | Response ♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| | Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood. | • Interview responsible personnel. | Our organisation maintains documented roles and responsibilities for all personnel involved in secure system development and maintenance activities within Azure. These responsibilities cover secure coding, vulnerability management, change control, deployment processes, and configuration management, and are communicated to ensure all individuals understand their duties.<br><br>Microsoft Azure provides the technical capabilities that support this requirement. Azure Role Based Access Control (RBAC) allows us to assign precise permissions aligned with each documented responsibility, ensuring that only authorised personnel can perform development, deployment, or configuration activities. Azure DevOps and GitHub provide role based pipelines and approval workflows that reinforce these assignments throughout the software development lifecycle.<br><br>Azure Activity Logs, Azure AD audit logs, and DevOps change histories provide visibility into who performed actions related to Requirement 6, enabling verification that responsibilities are being followed as documented. These logs also support periodic reviews to confirm that assigned roles remain appropriate and effective.<br><br>Through these capabilities, Azure enables us to clearly define, assign, and enforce roles and responsibilities related to secure system and software development, supporting compliance with PCI DSS Requirement 6.1.2. | | | | |

| 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 |
| **6.2** Bespoke and custom software are developed securely. | | | | | | | |
| **6.2.1** | Bespoke and custom software are developed securely, as follows:<br>• Based on industry standards and/or best practices for secure development.<br>• In accordance with PCI DSS (for example, secure authentication and logging).<br>• Incorporating consideration of information security issues during each stage of the software development lifecycle. | • Examine documented software development procedures. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | We do not store, process or transmit account data | | | | |
| **6.2.2** | Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:<br>• On software security relevant to their job function and development languages.<br>• Including secure software design and secure coding techniques.<br>• Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software. | • Examine documented software development procedures.<br>• Examine training records.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | We do not store, process or transmit 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 |
| **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:<br>• Code reviews ensure code is developed according to secure coding guidelines.<br>• Code reviews look for both existing and emerging software vulnerabilities.<br>Appropriate corrections are implemented prior to release. | • Examine documented software development procedures.<br>• Interview responsible personnel.<br>• Examine evidence of changes to bespoke and custom software. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement for code reviews applies to all bespoke and custom software (both internal and public facing), as part of the system development lifecycle.<br>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.<br>Code reviews may be performed using either manual or automated processes, or a combination of both. | | We do not store, process or transmit account data | | | | |
| **6.2.3.1** | If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:<br>• Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices.<br>• Reviewed and approved by management prior to release. | • Examine documented software development procedures.<br>• Interview responsible personnel.<br>• Examine evidence of changes to bespoke and custom software. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | Manual code reviews can be conducted by knowledgeable internal personnel or knowledgeable third-party personnel.<br>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. | | We do not store, process or transmit 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 |
| **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.<br>• 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. *(continued)* | | ☐ | ☐ | ☒ | ☐ | ☐ |
| **6.2.4** *(cont.)* | • 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. | | ☐ | ☐ | ☒ | ☐ | ☐ |

| 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 |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | We do not store, process or transmit account data | | | | |
| **6.3** Security vulnerabilities are identified and addressed. | | | | | | | |
| **6.3.1** | Security vulnerabilities are identified and managed as follows:<br>• New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).<br>• Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.<br>• Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.<br>• Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. | • Examine policies and procedures.<br>• Interview responsible personnel.<br>• Examine documentation.<br>• Observe processes. | ☒ | ☐ | ☐ | ☐ | ☐ |

| 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 |
| **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| This requirement is not achieved by, and is in addition to, performing vulnerability scans according to Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability. | | Our organisation maintains a formal process for identifying, evaluating, and risk ranking security vulnerabilities across all Azure hosted systems and software. Microsoft Azure provides the technical capabilities that support this requirement. Azure Defender for Cloud continuously monitors workloads and software components using Microsoft's global threat intelligence feeds, industry recognised vulnerability sources, and signals from international CERT teams. This enables early identification of new vulnerabilities affecting operating systems, middleware, application stacks, and third party components.<br><br>Azure's vulnerability assessment tools—such as integrated scanners for virtual machines, container registries, and SQL databases—provide detailed findings that include severity ratings aligned with industry best practices. These findings support our internal risk ranking process, ensuring that high risk and critical vulnerabilities are prioritised.<br><br>Azure DevOps and GitHub Advanced Security extend this capability to custom and bespoke software by providing dependency scanning, code scanning, and alerts for vulnerabilities in open source libraries. Azure Policy and Defender for Cloud recommendations ensure that vulnerability management requirements are consistently applied across all system components.<br><br>Through these capabilities, Azure enables us to identify, track, and risk rank vulnerabilities across all relevant software and system components, supporting compliance with PCI DSS Requirement 6.3.1. | | | | |

| 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 |
| **6.3.2** | An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management. | • Examine documentation.<br>• Interview personnel.<br>• | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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* | | We do not store, process or transmit 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 |
| **6.3.3** | All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:<br>• Patches/updates for critical vulnerabilities (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.<br>• All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity's assessment of the criticality of the risk to the environment as identified according to the risk ranking process at Requirement 6.3.1 | • Examine policies and procedures.<br>• Examine system components and related software.<br>• Compare list of security patches installed to recent vendor patch lists. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation ensures that all Azure hosted system components are protected from known vulnerabilities by applying applicable security patches and updates in accordance with our risk ranking process. Microsoft Azure provides the technical capabilities that support this requirement. Azure Update Management, Microsoft Defender for Cloud, and Azure Automation enable us to track, schedule, and deploy security patches across virtual machines and workloads.<br><br>Defender for Cloud continuously identifies missing patches and classifies them using industry recognised severity ratings, supporting our internal risk ranking process. Critical vulnerabilities are highlighted with clear remediation guidance, enabling us to meet the requirement to install critical patches within one month of release. Azure Policy enforces patch compliance baselines and alerts on systems that fall out of compliance.<br><br>Azure Monitor, Update Management logs, and Defender for Cloud recommendations provide evidence of patch deployment and allow us to compare installed patches against vendor release lists. These capabilities ensure that all applicable patches are applied within appropriate timeframes based on the criticality of the risk.<br><br>Through these mechanisms, Azure enables us to maintain timely and effective patching across all system components, supporting compliance with PCI DSS Requirement 6.3.3. | | | | |

| 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 |
| **6.4** 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:<br>• Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows:<br>– At least once every 12 months and after significant changes.<br>– By an entity that specializes in application security.<br>– Including, at a minimum, all common software attacks in Requirement 6.2.4.<br>– All vulnerabilities are ranked in accordance with Requirement 6.3.1.<br>– All vulnerabilities are corrected.<br>– The application is re-evaluated after the corrections.<br>**OR**<br>*(continued)* | • Examine documented processes.<br>• Interview personnel.<br>• Examine records of application security assessments<br>• Examine the system configuration settings and audit logs. | ☒ | ☐ | ☐ | ☐ | ☐ |
| **6.4.1** *(cont.)* | • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows:<br>– Installed in front of public-facing web applications to detect and prevent web-based attacks.<br>– Actively running and up to date as applicable.<br>– Generating audit logs.<br>– Configured to either block web-based attacks or generate an alert that is immediately investigated. | | | | | | |

| 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 |
| **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| This assessment is not the same as the vulnerability scans performed for Requirement 11.3.1 and 11.3.2.<br>This requirement will be superseded by Requirement 6.4.2 after 31 March 2025 when Requirement 6.4.2 becomes effective. | | Our organisation ensures that public facing web applications supporting Paritor Xperios are protected against known and emerging threats through a combination of regular application security assessments and automated protections. Microsoft Azure provides the technical capabilities that support this requirement. We conduct vulnerability assessments of public facing applications at least annually and after significant changes, using qualified application security specialists and approved scanning tools. Identified vulnerabilities are risk ranked in accordance with Requirement 6.3.1, remediated, and re evaluated to confirm resolution. Azure's integration with DevOps pipelines and third party testing tools supports this process by enabling consistent scanning and documentation. Through these measures, we ensure that Paritor Xperios public facing applications are reviewed, corrected, and re assessed in alignment with PCI DSS Requirement 6.4.1. | | | | |

| 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 |
| **6.4.2** | For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following:<br>• Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks.<br>• Actively running and up to date as applicable.<br>• Generating audit logs.<br>• Configured to either block web-based attacks or generate an alert that is immediately investigated. | • Examine the system configuration settings.<br>• Examine audit logs.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** *(continued)* | | *Describe results as instructed in "Requirement Responses" (page v) (continued)* | | | | |
| | This new requirement will replace Requirement 6.4.1 once its effective date is reached.<br>*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.* | | Our organisation deploys an automated technical solution in Azure to continually detect and prevent web based attacks against public facing Paritor Xperios applications. Azure Web Application Firewall (WAF), delivered through Azure Application Gateway or Azure Front Door, is installed in front of all public facing web applications and is configured to detect and block common web based attacks. Azure WAF is actively running, kept up to date with Microsoft maintained rule sets, and generates detailed audit logs that are ingested into Azure Monitor and Log Analytics for alerting and investigation. WAF policies are configured to block malicious traffic or generate alerts that are immediately reviewed by our security team. These capabilities ensure continuous, automated protection of Paritor Xperios web applications in alignment with PCI DSS Requirement 6.4.2. | | | | |

| 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 |
| **6.4.3** | 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.<br>• Interview responsible personnel.<br>• Examine inventory records.<br>• Examine system configurations. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | • A method is implemented to assure the integrity of each script. | | ☐ | ☐ | ☒ | ☐ | ☐ |
| | • An inventory of all scripts is maintained with written business or technical justification as to why each is necessary. | | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties.<br>This requirement also applies to scripts in the entity's webpage(s) that includes a TPSP's/payment processor's embedded payment page/form (for example, one or more inline frames or iframes).<br>This requirement does not apply to an entity for scripts in a TPSP's/payment processor's embedded payment page/form (for example, one or more iframes), where the entity includes a TPSP's/payment processor's payment page/form on its webpage.<br>Scripts in the TPSP's/payment processor's embedded payment page/form are the responsibility of the TPSP/payment processor to manage in accordance with this requirement.<br>*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.* | | We do not store, process or transmit 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 |
| **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:<br>• Reason for, and description of, the change.<br>• Documentation of security impact.<br>• Documented change approval by authorized parties.<br>• Testing to verify that the change does not adversely impact system security.<br>• For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.<br>• Procedures to address failures and return to a secure state. | • Examine documented change control procedures.<br>• Examine recent changes to system components and trace changes to change control documentation.<br>• Examine change control documentation. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We use Azure DevOps and GitHub which provide structured CI/CD pipelines with built-in change tracking, approvals, and automated testing. Infrastructure-as-code tools (ARM, Bicep, Terraform) ensure changes are version-controlled and testable. Azure Policy enforces deployment standards, while Defender for Cloud validates security posture pre- and post-deployment. Rollback is supported via deployment slots, snapshots, and backup integration. For Paritor Xperios, all custom code changes are scanned for OWASP vulnerabilities before release. | | | | |
| **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.<br>• Interview personnel.<br>• Observe the affected systems/networks. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | These significant changes should also be captured and reflected in the entity's annual PCI DSS scope confirmation activity per Requirement 12.5.2. | | We use Azure Resource Graph and Defender for Cloud whichprovide post-change validation of control coverage across VMs, databases, storage, and networking. Azure Policy ensures that required configurations (e.g., logging, encryption, anti-malware) are enforced. Change documentation is maintained via Azure DevOps and GitHub repositories. For Paritor Xperios, post-deployment checks confirm that PCI DSS controls remain effective and documented. | | | | |

| 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 |
| **6.5.3** | Pre-production environments are separated from production environments and the separation is enforced with access controls. | • Examine policies and procedures.<br>• Examine network documentation and configurations of network security controls.<br>• Examine access control settings. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We sue Azure Virtual Networks, Network Security Groups (NSGs), and Azure Firewall which enforce strict segmentation between environments. Azure AD (Entra ID) and RBAC restrict access to production resources. For Paritor Xperios, production and staging environments are isolated at the network and identity level, with access granted only to authorised roles. | | | | |
| **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.<br>• Observe processes.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | We use Azure AD supports role-based access with separate identities for development and production duties. Azure Privileged Identity Management (PIM) enforces just-in-time access and approval workflows. For Paritor Xperios, developers use non-privileged accounts for production access, and all elevated actions are logged and reviewed. | | | | |
| **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.<br>• Observe testing processes.<br>• Interview personnel.<br>• Examine pre-production test data. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We sue Azure Information Protection and Defender for Cloud classify and monitor sensitive data. Azure Policy blocks deployment of resources that violate data-handling rules. For Paritor Xperios, test environments use synthetic or anonymised data, and no live PANs are present outside the CDE. | | | | |

| 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 |
| **6.5.6** | Test data and test accounts are removed from system components before the system goes into production. | • Examine policies and procedures.<br>• Observe testing processes for both off-the-shelf software and in-house applications.<br>• Interview personnel.<br>• Examine data and accounts for recently installed or updated off-the-shelf software and in-house applications. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Azure DevOps release pipelines include pre-deployment scripts that purge test data and disable test accounts. Azure Policy and Defender for Cloud alert on non-compliant configurations. For Paritor Xperios, production deployments are validated to ensure no residual test artifacts remain. | | | | |

# 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:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>Known to all affected parties. | • Examine documentation.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **7.1.2** | Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood. | • Examine documentation.<br>• Interview responsible personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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:<br>• Appropriate access depending on the entity's business and access needs.<br>• Access to system components and data resources that is based on users' job classification and functions.<br>• The least privileges required (for example, user, administrator) to perform a job function. | • Examine documented policies and procedures.<br>• Interview personnel.<br>• Examine access control model settings. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |

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

| PCI DSS Requirement | | Expected Testing | Response ♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| **7.2.2** | Access is assigned to users, including privileged users, based on:<br>• Job classification and function.<br>• Least privileges necessary to perform job responsibilities. | • Examine policies and procedures.<br>• Examine user access settings, including for privileged users.<br>• Interview responsible management personnel.<br>• Interview personnel responsible for assigning access. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **7.2.3** | Required privileges are approved by authorized personnel. | • Examine policies and procedures.<br>• Examine user IDs and assigned privileges.<br>• Examine documented approvals. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **7.2.4** | All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:<br>• At least once every six months.<br>• To ensure user accounts and access remain appropriate based on job function.<br>• Any inappropriate access is addressed.<br>• Management acknowledges that access remains appropriate. | • Examine policies and procedures.<br>• Interview responsible personnel.<br>• Examine documented results of periodic reviews of user accounts. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies to all user accounts and related access privileges, including those used by personnel and third parties/vendors, and accounts used to access third-party cloud services.<br>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.<br>*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.* | | We do not store, process or transmit 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 |
| **7.2.5** | All application and system accounts and related access privileges are assigned and managed as follows:<br>• Based on the least privileges necessary for the operability of the system or application.<br>• Access is limited to the systems, applications, or processes that specifically require their use. | • Examine policies and procedures.<br>• Examine privileges associated with system and application accounts.<br>• Interview responsible personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | We do not store, process or transmit account data | | | | |
| **7.2.5.1** | All access by application and system accounts and related access privileges are reviewed as follows:<br>• 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).<br>• The application/system access remains appropriate for the function being performed.<br>• Any inappropriate access is addressed.<br>• Management acknowledges that access remains appropriate. | • Examine policies and procedures.<br>• Examine the targeted risk analysis.<br>• Interview responsible personnel.<br>• Examine documented results of periodic reviews of system and application accounts and related privileges. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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* | | We do not store, process or transmit 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 |
| **7.2.6** | All user access to query repositories of stored cardholder data is restricted as follows:<br>• Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges.<br>• Only the responsible administrator(s) can directly access or query repositories of stored CHD. | • Examine policies and procedures.<br>• Interview personnel.<br>• Examine configuration settings for querying repositories of stored cardholder data. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies to controls for user access to query repositories of stored cardholder data.<br>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. | | We do not store, process or transmit account data | | | | |
| **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.<br>• Examine configuration settings. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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.<br>• Examine configuration settings. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | Describe how the results of the testing performed support the selected response †: | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **7.3.3** | The access control system(s) is set to "deny all" by default. | • Examine vendor documentation.<br>• Examine configuration settings. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | Describe how the results of the testing performed support the selected response †: | | | | |
| | | | We do not store, process or transmit account data | | | | |

## *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:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | • Examine documentation.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We use Microsoft Azure which provides the governance and identity management framework that supports this requirement. Azure AD (Entra ID) is used to centrally manage user identities and authentication policies. Our organisation maintains documented procedures for user identification, access provisioning, and authentication, which are kept up to date and communicated to all affected personnel. Azure AD Conditional Access, MFA policies, and audit logging ensure that these procedures are actively enforced and understood. | | | | |
| **8.1.2** | Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood. | • Examine documentation.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Security policies and operational procedures related to user identification and authentication are documented and maintained within our compliance framework. Azure AD enforces these procedures through role assignments, access reviews, and policy enforcement. Azure Policy and Defender for Cloud provide visibility into compliance status. All relevant personnel are trained on these procedures, and changes are communicated through formal channels. | | | | |

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

| PCI DSS Requirement | | Expected Testing | Response♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| **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.<br>• Examine audit logs and other evidence. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | All users accessing Azure hosted components of Paritor Xperios are assigned unique Azure AD identities before access is permitted. No shared or generic accounts are used. Azure AD enforces unique identifiers and logs all authentication events. Access to system components and cardholder data is granted only after identity verification and role assignment. | | | | |
| **8.2.2** | Group, shared, or generic IDs, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows:<br>• ID use is prevented unless needed for an exceptional circumstance.<br>• Use is limited to the time needed for the exceptional circumstance.<br>• Business justification for use is documented.<br>• Use is explicitly approved by management.<br>• Individual user identity is confirmed before access to an account is granted.<br>• Every action taken is attributable to an individual user. | • Examine user account lists on system components and applicable documentation.<br>• Examine authentication policies and procedures.<br>• Interview system administrators. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | 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. | | Azure AD (Entra ID) enforces unique user identities for all access to Azure resources supporting Paritor Xperios. Shared or generic accounts are not used except in exceptional, documented circumstances. Azure AD Privileged Identity Management (PIM) ensures that any temporary elevation or exceptional access is time bound, explicitly approved, and fully attributable to an individual user. All actions taken under elevated or exceptional access are logged in Azure AD audit logs, ensuring accountability. | | | | |
| **8.2.3** | ***Additional requirement for service providers only:*** Service providers with remote access to customer premises use unique authentication factors for each customer premises. | • Examine authentication policies and procedures.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a service provider.<br>This requirement is not intended to apply to service providers accessing their own shared services environments, where multiple customer environments are hosted.<br>If service provider employees use shared authentication factors to remotely access customer premises, these factors must be unique per customer and managed in accordance with Requirement 8.2.2. | | We do not store, process or transmit account data | | | | |
| **8.2.4** | Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows:<br>• Authorized with the appropriate approval.<br>• Implemented with only the privileges specified on the documented approval. | • Examine documented authorizations across various phases of the account lifecycle (additions, modifications, and deletions).<br>• Examine system settings. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | This requirement applies to all user accounts, including employees, contractors, consultants, temporary workers, and third-party vendors. | | Azure AD Identity Governance ensures that user account creation, modification, and removal follow documented approval workflows. Access requests require authorisation, and Azure AD enforces only the privileges specified in the approval. All account lifecycle events are logged, and Azure AD Access Reviews ensure that permissions remain appropriate over time. | | | | |
| **8.2.5** | Access for terminated users is immediately revoked. | • Examine information sources for terminated users.<br>• Review current user access lists.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Azure AD enables immediate revocation of access by disabling or deleting user accounts as soon as employment or contract termination occurs. Conditional Access and token revocation ensure that any active sessions are terminated. Audit logs provide evidence that access was removed promptly. | | | | |
| **8.2.6** | Inactive user accounts are removed or disabled within 90 days of inactivity. | • Examine user accounts and last logon information.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Azure AD automatically tracks last sign in timestamps for all identities. Identity Governance policies and Access Reviews identify inactive accounts, which are disabled or removed within the required timeframe. Azure AD reporting provides evidence of inactivity and account status. | | | | |
| **8.2.7** | Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows:<br>• Enabled only during the time period needed and disabled when not in use.<br>• Use is monitored for unexpected activity. | • Interview responsible personnel.<br>• Examine documentation for managing accounts.<br>• Examine evidence. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **8.2.8** | If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session. | • Examine system configuration settings. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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 .<br>This requirement is not meant to prevent legitimate activities from being performed while the console/PC is unattended. | | We use Azure AD Conditional Access session controls which enforce idle timeout policies across Azure hosted applications and management interfaces. Administrators configure session timeouts so that inactive sessions require re authentication after the defined period. Azure portal, Azure DevOps, and other management tools support enforced re authentication to prevent unattended access. | | | | |
| **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:<br>• Something you know, such as a password or passphrase.<br>• Something you have, such as a token device or smart card.<br>• Something you are, such as a biometric element. | • Examine documentation describing the authentication factor(s) used.<br>• For each type of authentication factor used with each type of system component, observe the authentication process. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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.<br>This requirement does not supersede multi-factor authentication (MFA) requirements but applies to those in-scope systems not otherwise subject to MFA requirements.<br>A digital certificate is a valid option for "something you have" if it is unique for a particular user | | We use Azure AD which enforces strong authentication using passwords, MFA tokens, authenticator apps, FIDO2 security keys, or biometrics via Windows Hello for Business. All users and administrators authenticate using at least one valid factor, and MFA is required for privileged access. Authentication flows are logged and monitored | | | | |

| 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 |
| **8.3.2** | Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components. | • Examine vendor documentation<br>• Examine system configuration settings.<br>• Examine repositories of authentication factors.<br>• Examine data transmissions. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We use Azure AD which uses strong cryptography (TLS 1.2+ and modern cipher suites) to protect authentication data in transit. Credentials and authentication secrets are stored using secure hashing and encryption mechanisms. Azure AD never stores plaintext passwords or MFA secrets, and all authentication traffic is encrypted end to end | | | | |
| **8.3.3** | User identity is verified before modifying any authentication factor. | • Examine procedures for modifying authentication factors.<br>• Observe security personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We use Azure AD which requires identity verification before any authentication factor can be changed. This includes password resets, MFA device changes, and recovery method updates. Verification is enforced through self service password reset (SSPR) policies, MFA challenges, or administrator approved workflows. All changes are logged for audit purposes. | | | | |
| **8.3.4** | Invalid authentication attempts are limited by:<br>• Locking out the user ID after not more than 10 attempts.<br>• Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed. | • Examine system configuration settings. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | 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. | | We use Azure AD Smart Lockout which automatically locks accounts after repeated failed authentication attempts. Lockout thresholds and durations meet PCI DSS requirements, preventing brute force attacks while allowing legitimate users to recover securely. Lockout events are logged and monitored through Azure AD Identity Protection. | | | | |
| **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:<br>• Set to a unique value for first-time use and upon reset.<br>• Forced to be changed immediately after the first use. | • Examine procedures for setting and resetting passwords/passphrases.<br>• Observe security personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We use Azure AD which enforces unique temporary passwords for new accounts and password resets. Users are required to change the temporary password upon first login. Password reset procedures follow documented workflows, and Azure AD ensures that no default or shared passwords are used. All password related actions are logged for auditability. | | | | |

| 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 |
| **8.3.6** | If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:<br>• A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).<br>• Contain both numeric and alphabetic characters. | • Examine system configuration settings. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement is not intended to apply to:<br>• User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction .<br>• Application or system accounts, which are governed by requirements in section 8.6.<br>*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.*<br>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. | | We use Azure AD (Entra ID) which enforces password complexity policies that meet or exceed PCI DSS requirements. Passwords can be configured to require a minimum length of 12 characters and must include both alphabetic and numeric characters. Azure AD Password Protection also blocks weak or commonly used passwords. These policies apply to all user accounts accessing Azure hosted components of Paritor Xperios. | | | | |
| **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** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | We use Azure AD which enforces password history rules that prevent users from reusing recently used passwords. The platform supports blocking reuse of significantly more than four previous passwords, ensuring compliance with PCI DSS requirements. This prevents credential recycling and strengthens account security. | | | | |

| 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 |
| **8.3.8** | Authentication policies and procedures are documented and communicated to all users including:<br>• Guidance on selecting strong authentication factors.<br>• Guidance for how users should protect their authentication factors.<br>• Instructions not to reuse previously used passwords/passphrases.<br>• 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. | • Examine procedures.<br>• Interview personnel.<br>• Review authentication policies and procedures that are distributed to users.<br>• Interview users. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We use Azure AD which provides the technical enforcement for documented authentication policies, while our organisation maintains and communicates the associated procedures. Users receive guidance on selecting strong authentication factors, protecting credentials, avoiding password reuse, and reporting suspected compromise. Azure AD supports this through MFA enforcement, password protection policies, and user facing security notifications. | | | | |
| **8.3.9** | If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either:<br>• Passwords/passphrases are changed at least once every 90 days,<br>**OR**<br>• The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. | • Inspect system configuration settings. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement does not apply to in-scope system components where MFA is used.<br>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.<br>This requirement does not apply to service providers' customer accounts but does apply to accounts for service provider personnel. | | We do not store, process or transmit 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 |
| **8.3.10** | ***Additional requirement for service providers only:***<br>If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single-factor authentication implementation), then guidance is provided to customer users including:<br>• Guidance for customers to change their user passwords/passphrases periodically.<br>• Guidance as to when, and under what circumstances, passwords/passphrases are to be changed. | • Examine guidance provided to customer users. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a service provider.<br>This requirement does not apply to accounts of consumer users accessing their own payment card information.<br>This requirement for service providers will be superseded by Requirement 8.3.10.1 once 8.3.10.1 becomes effective. | | We do not store, process or transmit 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 |
| **8.3.10.1** | ***Additional requirement for service providers only:***<br>If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either:<br>• Passwords/passphrases are changed at least once every 90 days,<br>**OR**<br>• The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. | • Inspect system configuration settings. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a service provider.<br>This requirement does not apply to accounts of consumer users accessing their own payment card information.<br>*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.*<br>Until this requirement is effective on 31 March 2025, service providers may meet either Requirement 8.3.10 or 8.3.10.1. | | We do not store, process or transmit account data | | | | |
| **8.3.11** | Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used:<br>• Factors are assigned to an individual user and not shared among multiple users.<br>• Physical and/or logical controls ensure only the intended user can use that factor to gain access. | • Examine authentication policies and procedures.<br>• Interview security personnel.<br>• Examine system configuration settings and/or observe physical controls, as applicable. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **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.<br>• Observe administrator personnel logging into the CDE. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | We do not store, process or transmit 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 |
| **8.4.2** | MFA is implemented for all non-console access into the CDE. | • Examine network and/or system configurations.<br>• Observe personnel logging in to the CDE.<br>• Examine evidence. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| | | |
|---|---|---|
| | This requirement does not apply to:<br>• Application or system accounts performing automated functions.<br>• User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.<br>• User accounts that are only authenticated with phishing-resistant authentication factors.<br>MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3. Therefore, applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access. If an individual first connects to the entity's network via remote access, and then later initiates a connection into the CDE from within the network, per this requirement the individual would authenticate using MFA twice, once when connecting via remote access to the entity's network and once when connecting from the entity's network into the CDE.<br>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.<br>MFA for access into the CDE can be implemented at the network or system/application level; it does not have to be applied at both levels. For example, if MFA is used when a user connects to the CDE network, it does not have to be used when the user logs into each system or application within the CDE.<br>*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* | Azure AD (Entra ID) provides the multi factor authentication platform used to secure all non console access to Azure hosted components that support Paritor Xperios. MFA is enforced through Conditional Access policies, ensuring that any user accessing the Cardholder Data Environment (CDE) from outside the console must authenticate using at least two independent factors, such as a password plus an authenticator app, hardware token, or biometric factor.<br>Azure AD MFA applies consistently across all access paths, including Azure Portal access, remote administrative access, and application level access into CDE resources. Azure AD Identity Protection evaluates sign in risk and enforces MFA challenges when required. All MFA events are logged in Azure AD audit logs and can be monitored through Azure Monitor and Log Analytics to provide evidence of compliance.<br>Azure's MFA implementation meets PCI DSS expectations by ensuring that:<br>• MFA is required for all non console access into the CDE.<br>• MFA is applied regardless of whether access originates remotely or from within the network.<br>• MFA is enforced at the identity layer, covering all Azure hosted systems, applications, and administrative interfaces.<br>• Authentication events are fully logged and auditable.<br>Through these capabilities, Azure ensures that all non console access to Paritor Xperios CDE components is protected by strong multi factor authentication, supporting compliance with PCI DSS Requirement 8.4.2. |

| 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 |
| **8.4.3** | MFA is implemented for all remote access originating from outside the entity's network that could access or impact the CDE. | • Examine network and/or system configurations for remote access servers and systems.<br>• Observe personnel (for example, users and administrators) and third parties connecting remotely to the network. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | The requirement for MFA for remote access originating from outside the entity's network applies to all user accounts that can access the network remotely, where that remote access leads to or could lead to access into the CDE. This includes all remote access by personnel (users and administrators), and third parties (including, but not limited to, vendors, suppliers, service providers, and customers).<br>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.<br>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. | | Azure AD (Entra ID) enforces multi factor authentication for all remote access originating outside the organisation's network that could access or impact the CDE. Conditional Access policies require MFA for all sign ins from external networks, including administrators, internal users, and approved third parties. Azure AD Identity Protection evaluates sign in risk and triggers MFA challenges when suspicious activity is detected. All MFA events are logged in Azure AD audit logs and can be monitored through Azure Monitor and Log Analytics. This ensures that any remote access path into Azure hosted Paritor Xperios components is protected by strong MFA 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 |
| **8.5** Multi-factor authentication (MFA) systems are configured to prevent misuse. | | | | | | | |
| **8.5.1** | MFA systems are implemented as follows:<br>• The MFA system is not susceptible to replay attacks.<br>• 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.<br>• At least two different types of authentication factors are used.<br>• Success of all authentication factors is required before access is granted. | • Examine vendor system documentation.<br>• Examine system configurations for the MFA implementation.<br>• Interview responsible personnel and observe processes.<br>• Observe personnel logging into system components in the CDE.<br>• Observe personnel connecting remotely from outside the entity's network. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | Azure AD MFA requires at least two independent authentication factors, such as a password plus a possession factor (authenticator app, hardware token) or a biometric factor. Azure AD ensures that both factors must be successfully validated before access is granted. MFA cannot be bypassed by users unless an authorised administrator explicitly approves an exception, and such exceptions are logged. Azure AD's MFA implementation is resistant to replay attacks and uses strong cryptography to protect authentication 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 |
| **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:<br>• Interactive use is prevented unless needed for an exceptional circumstance.<br>• Interactive use is limited to the time needed for the exceptional circumstance.<br>• Business justification for interactive use is documented.<br>• Interactive use is explicitly approved by management.<br>• Individual user identity is confirmed before access to account is granted.<br>• Every action taken is attributable to an individual user. | • Examine application and system accounts that can be used for interactive login.<br>• Interview administrative personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | We use Azure AD (Entra ID) which enforces strict separation between human user accounts and application/system accounts. Application and system identities in Azure (Managed Identities, service principals, and app registrations) are not permitted for interactive login by default. If interactive use is ever required for an exceptional circumstance, Azure AD requires explicit administrator approval, time bound access via Privileged Identity Management (PIM), and full audit logging. All actions taken under elevated or exceptional access are attributable to an individual user through Azure AD audit logs and Azure Monitor. This ensures that interactive use is prevented unless justified, approved, time limited, and fully traceable. | | | | |

| 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 |
| **8.6.2** | 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.<br>• Examine system development procedures.<br>• 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** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | Stored passwords/passphrases are required to be encrypted in accordance with PCI DSS Requirement 8.3.2.<br>*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.* | | We use Azure which provides secure mechanisms that eliminate the need to store credentials in scripts or configuration files. Azure Key Vault stores application secrets, passwords, and connection strings using strong encryption and controlled access policies. Managed Identities allow Paritor Xperios services to authenticate to Azure resources without any stored credentials at all. Azure DevOps and GitHub Advanced Security include secret scanning tools that detect and prevent hard coded credentials in source code. These capabilities ensure that system and application account passwords are never embedded in scripts or code and are stored securely in accordance with PCI DSS requirements. | | | | |

| 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 |
| **8.6.3** | Passwords/passphrases for any application and system accounts are protected against misuse as follows:<br>• 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.<br>• Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases. | • Examine policies and procedures.<br>• Examine the targeted risk analysis.<br>• Interview responsible personnel.<br>• Examine system configuration settings. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | We use Azure Key Vault which enforces strong cryptographic protection for all stored secrets and supports automated secret rotation policies. Managed Identities remove the need for password rotation entirely by using certificate based authentication managed by Azure. For any remaining system accounts requiring passwords, Azure AD enforces complexity requirements and supports rotation aligned with the organisation's targeted risk analysis. Password changes can be triggered automatically upon suspected compromise, and all access to secrets is logged for audit purposes. These controls ensure that system and application account credentials are protected against misuse and rotated appropriately. | | | | |

## *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:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | • Examine documentation.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **9.1.2** | Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood. | • Examine documentation.<br>• Interview responsible personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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.<br>• Interview responsible personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| | **Applicability Notes**<br>This requirement does not apply to locations that are publicly accessible by consumers (cardholders). | | | | | | |

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

| PCI DSS Requirement | | Expected Testing | Response ♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| **9.2.1.1** | Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows:<br>• Entry and exit points to/from sensitive areas within the CDE are monitored.<br>• Monitoring devices or mechanisms are protected from tampering or disabling.<br>• Collected data is reviewed and correlated with other entries.<br>• 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.<br>• Observe the physical access control mechanisms and/or examine video cameras.<br>• Interview responsible personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **9.2.2** | Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility. | • Interview responsible personnel.<br>• Observe locations of publicly accessible network jacks. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **9.2.3** | Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted. | • Interview responsible personnel.<br>• Observe locations of hardware and lines. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **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:<br>• Identifying personnel.<br>• Managing changes to an individual's physical access requirements.<br>• Revoking or terminating personnel identification.<br>• Limiting access to the identification process or system to authorized personnel. | • Examine documented procedures.<br>• Observe identification methods, such as ID badges.<br>• Observe processes. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **9.3.1.1** | Physical access to sensitive areas within the CDE for personnel is controlled as follows:<br>• Access is authorized and based on individual job function.<br>• Access is revoked immediately upon termination.<br>• All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination. | • Observe personnel in sensitive areas within the CDE.<br>• Interview responsible personnel.<br>• Examine physical access control lists.<br>• Observe processes. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **9.3.2** | Procedures are implemented for authorizing and managing visitor access to the CDE, including:<br>• Visitors are authorized before entering.<br>• Visitors are escorted at all times.<br>• Visitors are clearly identified and given a badge or other identification that expires.<br>• Visitor badges or other identification visibly distinguishes visitors from personnel. | • Examine documented procedures.<br>• Observe processes when visitors are present in the CDE.<br>• Interview personnel.<br>• Observe the use of visitor badges or other identification. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **9.3.4** | Visitor logs are used to maintain a physical record of visitor activity both within the facility and within sensitive areas, including:<br>• The visitor's name and the organization represented.<br>• The date and time of the visit.<br>• The name of the personnel authorizing physical access.<br>• Retaining the log for at least three months, unless otherwise restricted by law. | • Examine the visitor logs.<br>• Interview responsible personnel.<br>• Examine visitor log storage locations. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **9.4.1.1** | Offline media backups with cardholder data are stored in a secure location. | • Examine documented procedures.<br>• Examine logs or other documentation.<br>• Interview responsible personnel at the storge location(s). | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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.<br>• Interview responsible personnel at the storage location(s). | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **9.4.2** | All media with cardholder data is classified in accordance with the sensitivity of the data. | • Examine documented procedures.<br>• Examine media logs or other documentation. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **9.4.3** | Media with cardholder data sent outside the facility is secured as follows:<br>• Media sent outside the facility is logged.<br>• Media is sent by secured courier or other delivery method that can be accurately tracked.<br>• Offsite tracking logs include details about media location. | • Examine documented procedures.<br>• Interview personnel.<br>• Examine records.<br>• Examine offsite tracking logs for all media. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **9.4.4** | Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals). | • Examine documented procedures.<br>• Examine offsite media tracking logs.<br>• Interview responsible personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | We do not store, process or transmit account data | | | | |
| **9.4.5** | Inventory logs of all electronic media with cardholder data are maintained. | • Examine documented procedures.<br>• Examine electronic media inventory logs.<br>• Interview responsible personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **9.4.5.1** | Inventories of electronic media with cardholder data are conducted at least once every 12 months. | • Examine documented procedures.<br>• Examine electronic media inventory logs.<br>• Interview responsible personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **9.4.6** | Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows:<br>• Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.<br>• Materials are stored in secure storage containers prior to destruction. | • Examine the media destruction policy.<br>• Observe processes.<br>• Interview personnel.<br>• Observe storage containers. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | We do not store, process or transmit account data | | | | |
| **9.4.7** | Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following:<br>• The electronic media is destroyed.<br>• The cardholder data is rendered unrecoverable so that it cannot be reconstructed. | • Examine the media destruction policy.<br>• Observe the media destruction process.<br>• Interview responsible personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | We do not store, process or transmit 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 |
| **9.5** Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution. | | | | | | | |
| **9.5.1** | 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:<br>• Maintaining a list of POI devices.<br>• Periodically inspecting POI devices to look for tampering or unauthorized substitution.<br>• Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices. | • Examine documented policies and procedures. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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). These requirements do not apply to:<br>• Components used only for manual PAN key entry.<br>• Commercial off-the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution. | | We do not store, process or transmit account data | | | | |
| **9.5.1.1** | An up-to-date list of POI devices is maintained, including:<br>• Make and model of the device.<br>• Location of device.<br>• Device serial number or other methods of unique identification. | • Examine the list of POI devices.<br>• Observe POI devices and device locations.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **9.5.1.2** | POI device surfaces are periodically inspected to detect tampering and unauthorized substitution. | • Examine documented procedures.<br>• Interview responsible personnel.<br>• Observe inspection processes. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **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. | • Examine the targeted risk analysis.<br>• Examine documented results of periodic device inspections.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | We do not store, process or transmit account data | | | | |
| **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:<br>• Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.<br>• Procedures to ensure devices are not installed, replaced, or returned without verification.<br>• Being aware of suspicious behavior around devices.<br>• Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel. | • Review training materials for personnel in POI environments.<br>• Interview responsible personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |

# 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 understood. | | | | | | | |
| **10.1.1** | All security policies and operational procedures that are identified in Requirement 10 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | • Examine documentation.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **10.1.2** | Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood. | • Examine documentation.<br>• Interview responsible personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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.<br>• Examine system configurations. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **10.2.1.1** | Audit logs capture all individual user access to cardholder data. | • Examine audit log configurations.<br>• Examine audit log data. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |

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

| PCI DSS Requirement | | Expected Testing | Response♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| **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.<br>• Examine audit log data. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **10.2.1.3** | Audit logs capture all access to audit logs. | • Examine audit log configurations.<br>• Examine audit log data. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **10.2.1.4** | Audit logs capture all invalid logical access attempts. | • Examine audit log configurations.<br>• Examine audit log data. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **10.2.1.5** | Audit logs capture all changes to identification and authentication credentials including, but not limited to:<br>• Creation of new accounts.<br>• Elevation of privileges.<br>• All changes, additions, or deletions to accounts with administrative access. | • Examine audit log configurations.<br>• Examine audit log data. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **10.2.1.6** | Audit logs capture the following:<br>• All initialization of new audit logs, and<br>• All starting, stopping, or pausing of the existing audit logs. | • Examine audit log configurations.<br>• Examine audit log data. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **10.2.1.7** | Audit logs capture all creation and deletion of system-level objects. | • Examine audit log configurations.<br>• Examine audit log data. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **10.2.2** | Audit logs record the following details for each auditable event:<br>• User identification.<br>• Type of event.<br>• Date and time.<br>• Success and failure indication.<br>• Origination of event.<br>• Identity or name of affected data, system component, resource, or service (for example, name and protocol). | • Interview responsible personnel.<br>• Examine audit log configurations.<br>• Examine audit log data. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account 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<br>• Examine system configurations and privileges. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **10.3.2** | Audit log files are protected to prevent modifications by individuals. | • Examine system configurations and privileges.<br>• Interview system administrators. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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.<br>• Examine monitored files.<br>• Examine results from monitoring activities. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **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:<br>• All security events.<br>• Logs of all system components that store, process, or transmit CHD and/or SAD.<br>• Logs of all critical system components.<br>• 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.<br>• Observe processes.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **10.4.1.1** | Automated mechanisms are used to perform audit log reviews. | • Examine log review mechanisms.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | We do not store, process or transmit account data | | | | |
| **10.4.2** | Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically. | • Examine security policies and procedures.<br>• Examine documented results of log reviews.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement is applicable to all other in-scope system components not included in Requirement 10.4.1. | | We do not store, process or transmit 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 |
| **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.<br>• Examine documented results of periodic log reviews.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | We do not store, process or transmit account data | | | | |
| **10.4.3** | Exceptions and anomalies identified during the review process are addressed. | • Examine security policies and procedures.<br>• Observe processes.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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.<br>• Examine configurations of audit log history.<br>• Examine audit logs.<br>• Interview personnel.<br>• Observe processes. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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. | • Examine system configuration settings. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | Keeping time-synchronization technology current includes managing vulnerabilities and patching the technology according to PCI DSS Requirements 6.3.1 and 6.3.3. | | We do not store, process or transmit 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 |
| **10.6.2** | Systems are configured to the correct and consistent time as follows:<br>• One or more designated time servers are in use.<br>• Only the designated central time server(s) receives time from external sources.<br>• Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC).<br>• The designated time server(s) accept time updates only from specific industry-accepted external sources.<br>• Where there is more than one designated time server, the time servers peer with one another to keep accurate time.<br>• Internal systems receive time information only from designated central time server(s). | • Examine system configuration settings for acquiring, distributing, and storing the correct time. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **10.6.3** | Time synchronization settings and data are protected as follows:<br>• Access to time data is restricted to only personnel with a business need.<br>• Any changes to time settings on critical systems are logged, monitored, and reviewed. | • Examine system configurations and time-synchronization settings and logs.<br>• Observe processes. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **10.7** Failures of critical security control systems are detected, reported, and responded to promptly. | | | | | | | |
| **10.7.1** | ***Additional requirement for service providers only:***<br>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:<br>• Network security controls.<br>• IDS/IPS.<br>• FIM.<br>• Anti-malware solutions.<br>• Physical access controls.<br>• Logical access controls.<br>• Audit logging mechanisms.<br>• Segmentation controls (if used). | • Examine documented processes.<br>• Observe detection and alerting processes.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a service provider.<br>This requirement will be superseded by Requirement 10.7.2 once as of 31 March 2025. | | We do not store, process or transmit 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 |
| **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:<br>• Network security controls.<br>• IDS/IPS.<br>• Change-detection mechanisms.<br>• Anti-malware solutions.<br>• Physical access controls.<br>• Logical access controls.<br>• Audit logging mechanisms.<br>• Segmentation controls (if used).<br>• Audit log review mechanisms.<br>• Automated security testing tools (if used). | • Examine documented processes.<br>• Observe detection and alerting processes.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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.<br>*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.* | | We do not store, process or transmit 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 |
| **10.7.3** | Failures of any critical security control systems are responded to promptly, including but not limited to:<br>• Restoring security functions.<br>• Identifying and documenting the duration (date and time from start to end) of the security failure.<br>• Identifying and documenting the cause(s) of failure and documenting required remediation.<br>• Identifying and addressing any security issues that arose during the failure.<br>• Determining whether further actions are required as a result of the security failure.<br>• Implementing controls to prevent the cause of failure from reoccurring.<br>• Resuming monitoring of security controls. | • Examine documented processes .<br>• Interview personnel.<br>• Examine records related to critical security control systems failures. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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.<br>*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.* | | We do not store, process or transmit account data | | | | |

## *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:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | • Examine documentation.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We use Azure's governance tools which help ensure that our documented security testing policies and procedures are consistently applied. Azure Policy enforces required configurations, while Defender for Cloud provides visibility into compliance with our documented standards. Azure AD (Entra ID) ensures that only authorised personnel can perform security testing activities, and audit logs provide evidence that procedures are followed. Our organisation maintains and communicates the policies, and Azure provides the enforcement and monitoring mechanisms that ensure they remain in use and effective | | | | |
| **11.1.2** | | • Examine documentation. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

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

| PCI DSS Requirement | | Expected Testing | Response ♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| | Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood. | • Interview responsible personnel. | We use Azure AD role based access control (RBAC) which ensures that responsibilities for security testing are clearly assigned and enforced. Only authorised personnel are granted permissions to run vulnerability scans, review security alerts, or modify security configurations. Azure Privileged Identity Management (PIM) provides just in time access for elevated roles, ensuring accountability and preventing unauthorised testing activity. Audit logs in Azure AD and Defender for Cloud provide evidence that assigned roles are being used appropriately and that responsibilities are understood by the individuals performing them. | | | | |
| **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:<br>• The presence of wireless (Wi-Fi) access points is tested for.<br>• All authorized and unauthorized wireless access points are detected and identified.<br>• Testing, detection, and identification occurs at least once every three months.<br>• If automated monitoring is used, personnel are notified via generated alerts. | • Examine policies and procedures.<br>• Examine the methodology(ies) in use and the resulting documentation.<br>• Interview personnel.<br>• Examine wireless assessment results.<br>• Examine configuration settings. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | The requirement applies even when a policy exists that prohibits the use of wireless technology.<br>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. | | We don't use wireless wifi access points | | | | |
| **11.2.2** | | • Examine documentation. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | An inventory of authorized wireless access points is maintained, including a documented business justification. | | We do not store, process or transmit account data | | | | |
| **11.3** External and internal vulnerabilities are regularly identified, prioritized, and addressed. | | | | | | | |
| **11.3.1** | Internal vulnerability scans are performed as follows:<br>• At least once every three months.<br>• Vulnerabilities that are either high-risk or critical (according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved.<br>• Rescans are performed that confirm all high-risk and all critical vulnerabilities (as noted above) have been resolved.<br>• Scan tool is kept up to date with latest vulnerability information.<br>• Scans are performed by qualified personnel and organizational independence of the tester exists. | • Examine internal scan report results.<br>• Examine scan tool configurations.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | It is not required to use a QSA or ASV to conduct internal vulnerability scans.<br>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. | | Azure provides the tooling and security intelligence that support our organisation's internal vulnerability scanning processes. Microsoft Defender for Cloud includes built in vulnerability assessment for virtual machines, container registries, databases, and other Azure resources. These assessments run continuously and are updated with Microsoft's global threat intelligence to ensure the latest vulnerabilities are detected.<br>Scan results identify high risk and critical vulnerabilities in line with our risk ranking process (Requirement 6.3.1). Azure Defender for Cloud provides clear remediation guidance, and rescans confirm that high risk and critical issues have been resolved. Azure Update Management and Azure Automation support timely patch deployment across affected systems. All scanning tools are kept current automatically by Microsoft, and our internal security team—independent from system owners—reviews and validates scan results.<br>These capabilities ensure that internal vulnerability scans for Paritor Xperios are performed regularly, high risk issues are prioritised, and remediation is verified | | | | |

| 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 |
| **11.3.1.1** | All other applicable vulnerabilities (those not ranked as high-risk vulnerabilities or critical vulnerabilities according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows:<br>• 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.<br>• Rescans are conducted as needed. | • Examine the targeted risk analysis.<br>• Interview responsible personnel.<br>• Examine internal scan report results or other documentation. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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.<br>*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.* | | Azure Defender for Cloud provides detailed vulnerability findings across all Azure resources, including lower risk issues. These findings feed into our organisation's targeted risk analysis, performed in accordance with Requirement 12.3.1. Azure's reporting tools allow us to classify vulnerabilities by severity, asset type, and exposure, enabling informed decisions about remediation timeframes.<br><br>Lower risk vulnerabilities are addressed according to the results of this risk analysis, and rescans are performed as needed to confirm resolution. Azure Policy and Defender for Cloud recommendations help ensure that lower risk configuration issues are tracked and remediated consistently. All scan results and remediation actions are logged for audit purposes.<br><br>Through these capabilities, Azure supports our structured approach to managing lower risk vulnerabilities for Paritor Xperios in alignment with PCI DSS Requirement 11.3.1.1. | | | | |

| 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 |
| **11.3.1.2** | Internal vulnerability scans are performed via authenticated scanning as follows: | | | | | | |
| | • Systems that are unable to accept credentials for authenticated scanning are documented. | • Examine documentation.<br>• Examine scan tool configurations.<br>• Examine scan report results.<br>• Interview personnel.<br>• 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** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | The authenticated scanning tools can be either host-based or network-based.<br>"Sufficient" privileges are those needed to access system resources such that a thorough scan can be conducted that detects known vulnerabilities.<br>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.<br>*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.* | | We use Microsoft Defender for Cloud which supports authenticated internal vulnerability scanning across Azure virtual machines, containers, and other system components. Scans are performed using credentials with sufficient privileges to detect known vulnerabilities. Where interactive login is possible, accounts used for scanning are managed in accordance with Requirement 8.2.2 — including documented justification, time bound access, and full auditability. Systems that cannot accept credentials (e.g., certain appliances or containers) are documented. Scan configurations and results are reviewed regularly to ensure coverage and effectiveness | | | | |

| 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 |
| **11.3.1.3** | Internal vulnerability scans are performed after any significant change as follows:<br>• Vulnerabilities that are either high-risk or critical (according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved.<br>• Rescans are conducted as needed.<br>• 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.<br>• Interview personnel.<br>• Examine internal scan and rescan report as applicable.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | Authenticated internal vulnerability scanning per Requirement 11.3.1.2 is not required for scans performed after significant changes. | | After any significant change to Azure hosted components supporting Paritor Xperios, internal vulnerability scans are performed using Defender for Cloud or approved third party tools. High risk and critical vulnerabilities are resolved in accordance with our risk ranking process (Requirement 6.3.1), and rescans confirm remediation. Scans are conducted by qualified personnel who are independent of the systems being changed. Azure DevOps and GitHub workflows support automated post deployment scanning, and scan results are logged and reviewed. | | | | |
| **11.3.2** | External vulnerability scans are performed as follows:<br>• At least once every three months.<br>• By a PCI SSC Approved Scanning Vendor (ASV)<br>• Vulnerabilities are resolved and *ASV Program Guide* requirements for a passing scan are met.<br>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.<br>• | ☒ | ☐ | ☐ | ☐ | ☐ |

| 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 |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | For the initial PCI DSS assessment against this requirement, it is not required that four passing scans be completed within 12 months if the assessor verifies: 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring scanning at least once every three months, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s).<br>However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred.<br>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.<br>Refer to the *ASV Program Guide* published on the PCI SSC website for scan customer responsibilities, scan preparation, etc. | | External vulnerability scans of Azure hosted public facing components are conducted at least quarterly by a PCI SSC Approved Scanning Vendor (ASV). Scan results are reviewed, and any identified vulnerabilities are remediated. Rescans are performed as needed to meet the ASV Program Guide requirements for a passing scan. Azure Firewall, Application Gateway, and Front Door configurations are included in the scan scope, and scan reports are retained for audit purposes. | | | | |
| **11.3.2.1** | External vulnerability scans are performed after any significant change as follows:<br>• Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved.<br>• Rescans are conducted as needed.<br>• 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.<br>• Interview personnel.<br>• Examine external scan, and as applicable rescan reports. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Following any significant change to public facing Azure components, external vulnerability scans are performed by our ASV. Vulnerabilities scored 4.0 or higher by CVSS are resolved, and rescans confirm remediation. Azure DevOps and change control documentation ensure that scan timing aligns with deployment events. Scans are conducted by qualified personnel with organisational independence, and scan results are reviewed and retained. | | | | |

| 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 |
| **11.4** 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:<br>• Industry-accepted penetration testing approaches.<br>• Coverage for the entire CDE perimeter and critical systems.<br>• Testing from both inside and outside the network.<br>• Testing to validate any segmentation and scope-reduction controls.<br>• Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4.<br>• Network-layer penetration tests that encompass all components that support network functions as well as operating systems.<br>• Review and consideration of threats and vulnerabilities experienced in the last 12 months.<br>• Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing.<br>• Retention of penetration testing results and remediation activities results for at least 12 months. | • Examine documentation.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** *(continued)* | | *Describe results as instructed in "Requirement Responses" (page v) (continued)* | | | | |

| 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 |
| **11.4.1** *(cont.)* | 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.<br>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. | | Azure provides the technical foundation and security controls that support our organisation's penetration testing methodology. Azure's shared responsibility model, security baselines, and Defender for Cloud threat intelligence inform the scope and approach of penetration testing. Azure's architecture enables testing of both internal and external attack surfaces, including network layer and application layer components. Segmentation controls (NSGs, Azure Firewall, VNET peering rules) can be validated through penetration testing to confirm that CDE boundaries are enforced. Azure logging (Azure Monitor, Log Analytics, Defender for Cloud) supports evidence collection and analysis. Our organisation maintains the documented methodology, while Azure provides the infrastructure, auditability, and security telemetry required to perform and retain penetration testing results for at least 12 months. | | | | |
| **11.4.2** | Internal penetration testing is performed:<br>• Per the entity's defined methodology.<br>• At least once every 12 months.<br>• After any significant infrastructure or application upgrade or change.<br>• By a qualified internal resource or qualified external third-party<br>• Organizational independence of the tester exists (not required to be a QSA or ASV). | • Examine scope of work.<br>• Examine results from the most recent external penetration test.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Azure enables internal penetration testing by providing full visibility into internal network paths, system components, and application endpoints. Azure's network segmentation, identity controls, and resource configurations can be tested by qualified internal or external testers with organisational independence. After significant changes to Paritor Xperios infrastructure (such as new deployments, architectural changes, or major updates), Azure's change tracking tools (Activity Logs, Resource Graph, DevOps pipelines) help identify what must be re tested. Azure's logging and monitoring provide evidence of testing and remediation activities | | | | |

| 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 |
| **11.4.3** | External penetration testing is performed:<br>• Per the entity's defined methodology.<br>• At least once every 12 months.<br>• After any significant infrastructure or application upgrade or change.<br>• By a qualified internal resource or qualified external third-party<br>• Organizational independence of the tester exists (not required to be a QSA or ASV). | • Examine scope of work.<br>• Examine results from the most recent external penetration test.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Azure supports external penetration testing by exposing only approved, public facing endpoints through Azure Front Door, Application Gateway, or public IPs. These components form the external attack surface that testers evaluate. Azure's DDoS protection, WAF, and network security controls can be validated through external testing. After significant changes to public facing components, Azure's deployment logs and change control processes ensure that external penetration testing is triggered appropriately. Azure's audit logs and Defender for Cloud findings support the documentation and review of test results. | | | | |
| **11.4.4** | Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows:<br>• In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1.<br>• Penetration testing is repeated to verify the corrections. | • Examine penetration testing results. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Azure Defender for Cloud provides continuous visibility into exploitable vulnerabilities identified during penetration testing. Remediation actions—such as patching, configuration changes, or WAF rule updates—are implemented through Azure Update Management, Azure Policy, and DevOps pipelines. Once remediation is complete, penetration testers can re test the affected Azure resources to verify that vulnerabilities have been fully resolved. Azure's logging and monitoring tools provide evidence of remediation and re testing, supporting compliance with PCI DSS requirements. | | | | |

| 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 |
| **11.4.5** | If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:<br>• At least once every 12 months and after any changes to segmentation controls/methods<br>• Covering all segmentation controls/methods in use.<br>• According to the entity's defined penetration testing methodology.<br>• Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.<br>• Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).<br>• Performed by a qualified internal resource or qualified external third party.<br>• Organizational independence of the tester exists (not required to be a QSA or ASV). | • Examine segmentation controls.<br>• Review penetration-testing methodology.<br>• Examine the results from the most recent penetration test.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Azure provides the network segmentation and isolation capabilities that support our organisation's penetration testing requirements. Segmentation between the CDE and non CDE systems is enforced using Azure Virtual Networks, Network Security Groups (NSGs), Azure Firewall, and route table controls. These controls define strict boundaries that limit access to CDE resources.<br><br>Penetration testers can validate these segmentation controls by testing traffic paths, firewall rules, and access restrictions across Azure network layers. Azure Monitor, Network Watcher, and Defender for Cloud provide visibility into segmentation behaviour and assist in verifying that isolation is effective. Our organisation performs penetration testing at least annually and after any changes to segmentation methods, using a qualified and independent tester. Azure's logging and configuration management ensure that segmentation controls are testable, traceable, and consistently enforced. | | | | |

| 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 |
| **11.4.6** | ***Additional requirement for service providers only:***<br>If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:<br>• At least once every six months and after any changes to segmentation controls/methods.<br>• Covering all segmentation controls/methods in use.<br>• According to the entity's defined penetration testing methodology.<br>• Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.<br>• Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).<br>• Performed by a qualified internal resource or qualified external third party.<br>• Organizational independence of the tester exists (not required to be a QSA or ASV). | • Examine the results from the most recent penetration test.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | This requirement applies only when the entity being assessed is a service provider. | | As a service provider, our organisation performs segmentation penetration testing at least every six months, in line with PCI DSS requirements. Azure's network architecture supports this by providing clearly defined segmentation boundaries that can be repeatedly tested. Azure Firewall, NSGs, VNET peering rules, and private endpoints form the segmentation controls that testers validate.<br><br>Azure Activity Logs, Defender for Cloud, and Network Watcher provide detailed telemetry that helps testers confirm whether segmentation is effective and whether any out of scope systems can reach the CDE. After any change to segmentation controls—such as firewall rule updates, network restructuring, or new services—Azure's change tracking and audit logs ensure that updated configurations are identified and re tested. Testing is performed by qualified personnel with organisational independence, and results are retained for review. | | | | |

| 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 |
| **11.4.7** | ***Additional requirement for multi-tenant service providers only:***<br>Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4. | • Examine evidence. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a multi-tenant service provider.<br>To meet this requirement, multi-tenant service providers may either:<br>• Provide evidence to its customers to show that penetration testing has been performed according to Requirements 11.4.3 and 11.4.4 on the customers' subscribed infrastructure,<br>**OR**<br>• Provide prompt access to each of its customers, so customers can perform their own penetration testing.<br>Evidence provided to customers can include redacted penetration testing results but needs to include sufficient information to prove that all elements of Requirements 11.4.3 and 11.4.4 have been met on the customer's behalf. Refer also to *Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers.*<br>*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.* | | Azure provides the technical environment and controls that enable our organisation, as a service provider, to support customer penetration testing requirements. Azure's shared responsibility model allows us to provide customers with evidence of penetration testing performed on Azure hosted Paritor Xperios components, including redacted reports demonstrating that external penetration testing has been completed in accordance with Requirements 11.4.3 and 11.4.4. Azure's network architecture also allows customers to conduct their own penetration testing of permitted public facing endpoints, subject to Microsoft's documented penetration testing rules of engagement. Azure logging and monitoring ensure that any customer initiated testing is visible, controlled, and does not impact service integrity. These capabilities allow us to meet customer support obligations as a multi tenant service provider. | | | | |

| 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 |
| **11.5** 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:<br>• All traffic is monitored at the perimeter of the CDE.<br>• All traffic is monitored at critical points in the CDE.<br>• Personnel are alerted to suspected compromises.<br>• All intrusion-detection and prevention engines, baselines, and signatures are kept up to date. | • Examine system configurations and network diagrams.<br>• Examine system configurations.<br>• Interview responsible personnel.<br>• Examine vendor documentation. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Azure provides multiple layers of intrusion detection and intrusion prevention capabilities that protect the Paritor Xperios environment. Azure Firewall, Network Security Groups (NSGs), and Azure DDoS Protection monitor and control traffic at the CDE perimeter and critical internal points. Microsoft Defender for Cloud continuously analyses network traffic, system behaviour, and threat signals to detect suspicious activity. Alerts are generated in real time and integrated into Azure Monitor and Microsoft Sentinel for investigation and response. All IDS/IPS engines, signatures, and baselines are automatically updated by Microsoft, ensuring continuous protection without manual maintenance. These capabilities ensure that intrusions are detected, prevented, and escalated promptly. | | | | |
| **11.5.1.1** | ***Additional requirement for service providers only:***<br>Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels. | • Examine documentation.<br>• Examine configuration settings.<br>• Examine the incident-response plan.<br>• Interview responsible personnel.<br>• Observe processes. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | This requirement applies only when the entity being assessed is a service provider.<br>*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* | | Azure's advanced threat detection capabilities identify and block covert malware communication channels, including command and control traffic, anomalous outbound connections, and suspicious lateral movement. Microsoft Defender for Cloud and Microsoft Sentinel use machine learning, behavioural analytics, and Microsoft's global threat intelligence to detect hidden or encrypted malware communication patterns. Alerts are generated automatically and integrated into our incident response process. Azure Firewall Premium provides TLS inspection and threat intelligence based filtering to prevent malicious outbound communication. These capabilities ensure that covert malware channels are detected, alerted on, and addressed in accordance with PCI DSS requirements. | | | | |

| 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 |
| **11.5.2** | A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows:<br>• To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files.<br>• To perform critical file comparisons at least once weekly. | • Examine system settings for the change-detection mechanism.<br>• Examine monitored files.<br>• Examine results from monitoring activities. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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). | | Azure provides the tooling and monitoring capabilities needed to detect unauthorised changes to critical system files. Microsoft Defender for Cloud includes File Integrity Monitoring (FIM) functionality that tracks changes, additions, and deletions to critical operating system files, configuration files, and application components. FIM alerts are generated in real time and forwarded to Azure Monitor or Microsoft Sentinel for investigation.<br><br>Critical files for Paritor Xperios are defined as part of our configuration hardening process, and Azure's monitoring agents evaluate these files at least weekly, in line with PCI DSS expectations. All FIM events are logged, retained, and reviewed to ensure that any unexpected modification is detected and responded to promptly | | | | |

| 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 |
| **11.6** 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 security-impacting HTTP headers and the script contents of payment pages as received by the consumer browser. | • Examine system settings and mechanism configuration settings.<br>• Examine monitored payment pages.<br>• Examine results from monitoring activities.<br>• Examine the mechanism configuration settings.<br>• Examine configuration settings.<br>• Interview responsible personnel.<br>• If applicable, examine the targeted risk analysis. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | • The mechanism is configured to evaluate the received HTTP headers and payment pages. | | ☒ | ☐ | ☐ | ☐ | ☐ |
| | • The mechanism functions are performed as follows:<br>– At least once weekly,<br>**OR**<br>– 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** *(continued)* | | *Describe results as instructed in "Requirement Responses" (page v) (continued)* | | | | |

| 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 |
| | This requirement also applies to entities with a webpage(s) that includes a TPSP's/payment processor's embedded payment page/form (for example, one or more inline frames or iframes.)<br>This requirement does not apply to an entity for scripts in a TPSP's/payment processor's embedded payment page/form (for example, one or more iframes), where the entity includes a TPSP's/payment processor's payment page/form on its webpage.<br>Scripts in the TPSP's/payment processor's embedded payment page/form are the responsibility of the TPSP/payment processor to manage in accordance with this requirement.<br>The intention of this requirement is not that an entity installs 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.<br>*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.* | Azure provides the infrastructure and monitoring capabilities that support detection of unauthorised changes to payment page content and security impacting HTTP headers. Azure Front Door and Application Gateway integrate with Web Application Firewall (WAF) to detect and block malicious script injection, header manipulation, and tampering attempts. Defender for Cloud Apps and Microsoft Sentinel provide behavioural analytics and alerting for suspicious modifications or indicators of compromise.<br>Where Paritor Xperios hosts or serves payment pages, Azure based monitoring tools evaluate the delivered page content and headers at defined intervals, or at least weekly, depending on the targeted risk analysis. Alerts are generated for any unexpected changes, and logs are retained for audit and incident response purposes. If Paritor Xperios does not directly host payment pages, this requirement is marked as Not Applicable, but Azure still provides the capability if needed. | | | | |

# 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:<br>• Established.<br>• Published.<br>• Maintained.<br>• Disseminated to all relevant personnel, as well as to relevant vendors and business partners. | • Examine the information security policy.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Azure's governance tools support the implementation of our security policy by enforcing configuration baselines, access controls, and monitoring standards. Azure AD (Entra ID) ensures that only authorised personnel can access policy documents and compliance dashboards. Our organisation maintains and distributes the policy through secure internal channels, and Azure's audit logs confirm that policy driven controls are in use | | | | |
| **12.1.2** | The information security policy is:<br>• Reviewed at least once every 12 months.<br>• Updated as needed to reflect changes to business objectives or risks to the environment | • Examine the information security policy.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Azure's compliance and security dashboards provide continuous visibility into control effectiveness, helping inform our annual policy review. Defender for Cloud and Microsoft Purview track changes in risk posture and regulatory requirements, prompting updates to our policy when needed. Azure's change tracking and audit capabilities support the documentation of policy revisions and ensure alignment with current business objectives. | | | | |
| **12.1.3** | | | ☒ | ☐ | ☐ | ☐ | ☐ |

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

| PCI DSS Requirement | | Expected Testing | Response ♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| | 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.<br>• Interview responsible personnel.<br>• Examine documented evidence. | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Azure AD role based access control (RBAC) ensures that security responsibilities are clearly assigned and enforced. Each role within Azure—such as Security Administrator, Compliance Manager, or Application Owner—is mapped to documented responsibilities in our security policy. Azure Privileged Identity Management (PIM) enforces just in time access and approval workflows, ensuring accountability. Personnel acknowledge their responsibilities through onboarding and periodic training. | | | | |
| **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. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Responsibility for information security is formally assigned to a designated member of executive management. Azure's compliance tools, including Defender for Cloud and Microsoft Purview, provide dashboards and reporting that support executive oversight. The assigned individual has access to Azure's security posture summaries and risk alerts, enabling informed decision making and accountability. | | | | |
| **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:<br>• Explicit approval by authorized parties.<br>• Acceptable uses of the technology.<br>• List of products approved by the company for employee use, including hardware and software. | • Examine acceptable use policies.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | 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. | | Azure AD Conditional Access policies enforce acceptable use standards for end user technologies such as laptops, mobile devices, and remote access tools. Our documented acceptable use policy defines approved hardware and software, usage guidelines, and approval processes. Azure Intune (Endpoint Manager) manages device compliance, ensuring that only authorised and secure devices can access Azure resources. Logs and alerts confirm policy enforcement. | | | | |
| **12.3** Risks to the cardholder data environment are formally identified, evaluated, and managed. | | | | | | | |
| **12.3.1** | For each PCI DSS requirement that specifies completion of a targeted risk analysis, the analysis is documented and includes:<br>• Identification of the assets being protected.<br>• Identification of the threat(s) that the requirement is protecting against.<br>• Identification of factors that contribute to the likelihood and/or impact of a threat being realized.<br>• Resulting analysis that determines, and includes justification for, how the frequency or processes defined by the entity to meet the requirement minimize the likelihood and/or impact of the threat being realized.<br>• 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<br>• Performance of updated risk analyses when needed, as determined by the annual review. | • Examine documented policies and procedures. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | *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.* | | We do not store, process or transmit account data | | | | |
| **12.3.2** | ***This requirement is specific to the customized approach and does not apply to entities completing a self-assessment questionnaire.*** | | | | | | |
| **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:<br>• An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used.<br>• Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use.<br>• Documentation of a plan to respond to anticipated changes in cryptographic vulnerabilities. | • Examine documentation.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | The requirement applies to all cryptographic cipher suites and protocols used to meet PCI DSS requirements, including, but not limited to, those used to render PAN unreadable in storage and transmission, to protect passwords, and as part of authenticating access.<br>*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.* | | We do not store, process or transmit 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 |
| **12.3.4** | Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following:<br>• Analysis that the technologies continue to receive security fixes from vendors promptly.<br>• Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance.<br>• 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.<br>• 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.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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* | | We do not store, process or transmit 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 |
| **12.4** PCI DSS compliance is managed. | | | | | | | |
| **12.4.1** | ***Additional requirement for service providers only:***<br>Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include:<br>• Overall accountability for maintaining PCI DSS compliance.<br>• Defining a charter for a PCI DSS compliance program and communication to executive management. | • Examine documentation. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a service provider.<br>Executive management may include C-level positions, board of directors, or equivalent. The specific titles will depend on the particular organizational structure.<br>Responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization. | | Azure provides the governance, monitoring, and compliance tooling that enables executive management to maintain oversight and accountability for PCI DSS compliance. Azure Policy, Microsoft Defender for Cloud, and Microsoft Purview Compliance Manager provide dashboards and automated reporting that give leadership visibility into the security posture of all Azure hosted components supporting Paritor Xperios. These tools help executive management define and maintain a formal PCI DSS compliance charter, assign ownership, and track adherence to required controls. Azure's audit logs and compliance insights support regular reporting to leadership, ensuring that accountability for protecting cardholder data is clearly established and maintained. | | | | |

| 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 |
| **12.4.2** | ***Additional requirement for service providers only:***<br>Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks.<br>• Daily log reviews.<br>• Configuration reviews for network security controls.<br>• Applying configuration standards to new systems.<br>• Responding to security alerts.<br>• Change-management processes. | • Examine documented policies and procedures.<br>• Interview responsible personnel.<br>• Examine records of reviews. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | This requirement applies only when the entity being assessed is a service provider. | | Azure's governance and monitoring capabilities enable structured quarterly reviews of operational security tasks. Azure Monitor, Log Analytics, and Microsoft Sentinel provide detailed logs for daily security reviews, alert handling, and incident response. Azure Policy and Defender for Cloud supply evidence of configuration compliance, network security control reviews, and adherence to baseline standards. Azure AD (Entra ID) and Privileged Identity Management (PIM) provide audit trails for access reviews, change management activities, and privileged operations.<br><br>Quarterly reviews are performed by personnel independent of the individuals carrying out the daily tasks, and Azure's reporting tools make it straightforward to validate that:Daily log reviews are being completed. Network security configurations follow approved standards. New systems are deployed with required security baselines. Security alerts are triaged and resolve. Change management processes are followed<br><br>Azure's built in auditability ensures that review records are complete, consistent, and retained for compliance evidence. | | | | |

| 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 |
| **12.4.2.1** | ***Additional requirement for service providers only:***<br>Reviews conducted in accordance with Requirement 12.4.2 are documented to include:<br>• Results of the reviews.<br>• Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2.<br>• Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program. | • Examine documentation from the reviews. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a service provider. | | Quarterly compliance reviews are formally documented and retained as part of our PCI DSS governance process. Azure's monitoring and audit capabilities provide the evidence base for these reviews, including log review records, configuration baseline reports, alert handling documentation, and change management evidence. Reviews are performed by personnel independent of those carrying out the daily operational tasks, ensuring objectivity. Azure Monitor, Microsoft Sentinel, Defender for Cloud, and Azure Policy supply the artefacts needed to validate that required security tasks are being performed consistently and in accordance with documented procedures. | | | | |
| **12.5** PCI DSS scope is documented and validated. | | | | | | | |
| **12.5.1** | | • Examine the inventory.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current. | | Azure Resource Graph and Azure Inventory provide real time visibility into all system components deployed within the Azure environment. These tools allow us to maintain an accurate inventory of virtual machines, storage accounts, databases, network components, and security controls that fall within PCI DSS scope. Inventory records are updated automatically as resources are added, modified, or removed. This ensures that our PCI DSS system component inventory remains complete, accurate, and aligned with the current environment. | | | | |
| **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. | • Examine documented results of scope reviews.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | ***At a minimum, the scoping validation includes:*** | | | | | | |
| | • 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). | • Examine documented results of scope reviews. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | • Updating all data-flow diagrams per requirement 1.2.4. *(continued)* | | ☒ | ☐ | ☐ | ☐ | ☐ |
| **12.5.2** *(cont.)* | • 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. | | ☒ | ☐ | ☐ | ☐ | ☐ |

| 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 |
| • 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** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| 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. | | Azure's governance and monitoring capabilities support annual and change driven scope validation. Azure Activity Logs, DevOps pipelines, and change management processes identify when significant changes occur, triggering a scope review. During annual reviews, Azure Resource Graph and Defender for Cloud are used to confirm:<br>• All locations where cardholder data could be stored, processed, or transmitted<br>• All system components connected to or supporting the CDE<br>• All segmentation controls (NSGs, Azure Firewall, VNET boundaries, private endpoints)<br>• All inbound and outbound connections to the CDE<br>• Any changes in architecture, services, or integrations<br>These reviews ensure that the documented PCI DSS scope remains accurate and that segmentation continues to isolate the CDE from out of scope systems. | | | | |

| 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 |
| **12.5.2.1** | **Additional requirement for service providers only:**<br>PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment.<br>At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2. | • Examine documented results of scope reviews.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a service provider.<br>*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.* | | Azure's governance and monitoring tools support semi annual scope validation. Azure Resource Graph, Defender for Cloud, and Azure Policy provide visibility into all in scope system components, segmentation controls, and data flows. Scope reviews are documented and triggered both on a six month cadence and after any significant architectural or operational change. Azure's audit logs and change tracking features ensure that scope reviews are based on current infrastructure and accurately reflect the CDE boundaries. | | | | |
| **12.5.3** | ***Additional requirement for service providers only:***<br>Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management. | • Examine policies and procedures.<br>• Interview responsible personnel.<br>• Examine documentation (for example, meeting minutes). | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | This requirement applies only when the entity being assessed is a service provider.<br>*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.* | | Significant changes to organisational structure—such as team restructuring, role reassignment, or service ownership changes—trigger an internal review of PCI DSS scope and control applicability. Azure AD (Entra ID) and Defender for Cloud provide visibility into access roles, control enforcement, and resource ownership. Review outcomes are documented and communicated to executive management, ensuring that PCI DSS scope remains accurate and that control responsibilities are reassigned as needed. | | | | |
| **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. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Our organisation maintains a formal security awareness program that educates personnel on the information security policy, PCI DSS responsibilities, and their role in protecting cardholder data. Azure AD and Microsoft 365 provide secure access to training materials, policy documents, and acknowledgement workflows. Azure's audit capabilities ensure that access to CDE systems is restricted to trained and authorised personnel. | | | | |
| **12.6.2** | The security awareness program is:<br>• Reviewed at least once every 12 months, and<br>• Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's cardholder data and/or sensitive authentication data, or the information provided to personnel about their role in protecting cardholder data. | • Examine security awareness program content.<br>• Examine evidence of reviews.<br>• Interview personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |

| 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 |
| | *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.* | | The security awareness program is reviewed annually and updated to reflect emerging threats and vulnerabilities. Azure Defender for Cloud and Microsoft threat intelligence inform updates to training content, ensuring relevance. Review records and updated materials are retained, and Azure AD ensures that only current, approved content is distributed to personnel. | | | | |
| **12.6.3** | Personnel receive security awareness training as follows:<br>• Upon hire and at least once every 12 months.<br>• Multiple methods of communication are used.<br>• Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures. | • Examine security awareness program records.<br>• Interview applicable personnel.<br>• Examine the security awareness program materials.<br>• Examine personnel acknowledgements. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | Security awareness training is delivered upon hire and at least annually via multiple channels, including online modules, email campaigns, and team briefings. Personnel acknowledge receipt and understanding of the information security policy through Microsoft 365 workflows. Azure AD tracks training completion and access rights, ensuring that only trained personnel can access in scope systems. | | | | |

| 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 |
| **12.6.3.1** | Security awareness training includes awareness of threats and vulnerabilities that could impact the security of cardholder data and/or sensitive authentication data, including but not limited to:<br>• Phishing and related attacks.<br>• Social engineering. | • Examine security awareness training content. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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.<br>*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.* | | Security awareness training includes targeted modules on phishing, social engineering, and related attack vectors. Microsoft Defender for Office 365 provides simulated phishing campaigns and user level reporting, reinforcing awareness. Azure Sentinel and Defender for Cloud Apps monitor for behavioural indicators of compromise, and training materials are updated to reflect current threat trends | | | | |
| **12.6.3.2** | Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1. | • Examine security awareness training content. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | Our security awareness training program includes clear guidance on the acceptable use of end user technologies, aligned with Requirement 12.2.1. Topics include secure use of laptops, mobile devices, remote access tools, email, and internet services. Azure AD Conditional Access and Intune enforce acceptable use policies, and training materials are distributed via Microsoft 365. Personnel acknowledge their understanding annually, and updates are issued when technology or policy changes occur. | | | | |

| 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 |
| **12.7** 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. | • Interview responsible Human Resource department management personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | We do not store, process or transmit account data | | | | |
| **12.8** Risk to information assets associated with third-party service provider (TPSP) relationships is managed. | | | | | | | |
| **12.8.1** | A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided. | • Examine policies and procedures.<br>• Examine list of TPSPs. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | No account data is maintained | | | | |
| **12.8.2** | Written agreements with TPSPs are maintained as follows:<br>• Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE.<br>• Written agreements include acknowledgments from TPSPs that TPSPs are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that the TPSP could impact the security of the entity's cardholder data and/or sensitive authentication data. | • Examine policies and procedures.<br>• Examine written agreements with TPSPs. | ☐ | ☐ | ☒ | ☐ | ☐ |

| 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 |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | The exact wording of an agreement will depend on the details of the service being provided, and the responsibilities assigned to each party. The agreement does not have to include the exact wording provided in this requirement.<br>The TPSP's written acknowledgment is a confirmation that states the TPSP is responsible for the security of the account data it may store, process, or transmit on behalf of the customer or to the extent the TPSP may impact the security of a customer's cardholder data and/or sensitive authentication data.<br>Evidence that a TPSP is meeting PCI DSS requirements (is not the same as a written acknowledgment specified in this requirement. For example, a PCI DSS Attestation of Compliance (AOC), a declaration on a company's website, a policy statement, a responsibility matrix, or other evidence not included in a written agreement is not a written acknowledgment. | | No account data is maintained | | | | |
| **12.8.3** | An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement. | • Examine policies and procedures.<br>• Examine evidence.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | A structured TPSP onboarding process is in place to ensure that any third party provider with potential impact on the CDE is properly assessed before engagement. This process includes reviewing the provider's security posture, validating their PCI DSS compliance status, and assessing their technical and operational controls. Azure's governance tools—such as Microsoft Defender for Cloud, Purview Compliance Manager, and Azure AD enterprise application insights—help identify integration points and potential risks. Documentation of due diligence activities is retained and reviewed by the compliance and procurement teams before any TPSP is approved. | | | | |

| 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 |
| **12.8.4** | A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months. | • Examine policies and procedures.<br>• Examine documentation.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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. | | We maintain an annual review cycle to confirm the PCI DSS compliance status of all TPSPs that could affect the security of cardholder data. This includes collecting updated Attestations of Compliance (AOCs), reviewing SOC 2 reports where applicable, and validating that the provider continues to meet required security obligations. Azure's built in compliance reporting and Microsoft's Trust Center provide up to date evidence for Microsoft managed services. Review results are documented and retained as part of our PCI DSS governance program. | | | | |
| **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.<br>• Examine documentation.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | A responsibility matrix is maintained that clearly identifies which PCI DSS requirements are fulfilled by each TPSP, which are fulfilled by Paritor, and which are shared. This matrix is based on the shared responsibility model for cloud services and is updated whenever services or integrations change. Azure's documentation, including service specific responsibility models, informs this mapping. The matrix ensures that all PCI DSS requirements are accounted for and that no control gaps exist between Paritor and its service providers. | | | | |

| 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 |
| **12.9** Third-party service providers (TPSPs) support their customers' PCI DSS compliance. | | | | | | | |
| **12.9.1** | ***Additional requirement for service providers only:***<br>TPSPs provide written agreements to customers that include acknowledgments that TPSPs are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that the TPSP could impact the security of the customer's cardholder data and/or sensitive authentication data. | • Examine TPSP policies and procedures.<br>• Examine templates used for written agreements. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a service provider.<br>The exact wording of an agreement will depend on the details of the service being provided, and the responsibilities assigned to each party. The agreement does not have to include the exact wording provided in this requirement.<br>The TPSP's written acknowledgment is a confirmation that states the TPSP is responsible for the security of the account data it may store, process, or transmit on behalf of the customer or to the extent the TPSP may impact the security of a customer's cardholder data and/or sensitive authentication data.<br>Evidence that a TPSP is meeting PCI DSS requirements is not the same as a written agreement specified in this requirement. For example, a PCI DSS Attestation of Compliance (AOC), a declaration on a company's website, a policy statement, a responsibility matrix, or other evidence not included in a written agreement is not a written acknowledgment. | | Azure provides PCI DSS–validated infrastructure and publishes its Attestation of Compliance and PCI responsibility matrix through the Microsoft Service Trust Portal. These documents describe Azure's PCI certified controls, operational procedures, and validated services. | | | | |

| 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 |
| **12.9.2** | ***Additional requirement for service providers only:***<br>TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request:<br>• PCI DSS compliance status information (Requirement 12.8.4).<br>• Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5), for any service the TPSP provides that meets a PCI DSS requirement(s) on behalf of customers or that can impact security of customers' cardholder data and/or sensitive authentication data. | • Examine policies and procedures. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a service provider. | | We do not store, process or transmit 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 |
| **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:<br>• 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.<br>• Incident response procedures with specific containment and mitigation activities for different types of incidents.<br>• Business recovery and continuity procedures.<br>• Data backup processes.<br>• Analysis of legal requirements for reporting compromises.<br>• Coverage and responses of all critical system components.<br>• Reference or inclusion of incident response procedures from the payment brands. | • Examine the incident response plan.<br>• Interview personnel.<br>• Examine documentation from previously reported incidents. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **12.10.2** | At least once every 12 months, the security incident response plan is:<br>• Reviewed and the content is updated as needed.<br>• Tested, including all elements listed in Requirement 12.10.1. | • Interview personnel.<br>• Examine documentation. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **12.10.3** | Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents. | • Interview responsible personnel.<br>• Examine documentation. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **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.<br>• Examine training documentation. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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. | • Examine the targeted risk analysis. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | We do not store, process or transmit account data | | | | |
| **12.10.5** | The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to:<br>• Intrusion-detection and intrusion-prevention systems.<br>• Network security controls.<br>• Change-detection mechanisms for critical files.<br>• 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.*<br>• Detection of *unauthorized* wireless access points. | • Examine documentation.<br>• Observe incident response processes. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *The bullet above (for monitoring and responding to alerts from a change- and tamper-detection 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.* | | We do not store, process or transmit 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 |
| **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.<br>• Examine the security incident response plan.<br>• Interview responsible personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **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:<br>• 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.<br>• Identifying whether sensitive authentication data is stored with PAN.<br>• Determining where the account data came from and how it ended up where it was not expected.<br>• Remediating data leaks or process gaps that resulted in the account data being where it was not expected. | • Examine documented incident response procedures.<br>• Interview personnel.<br>• Examine records of response actions. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | We do not store, process or transmit account data | | | | |

# Appendix A: Additional PCI DSS Requirements

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

| 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 |
| **A1.1** Multi-tenant service providers protect and separate all customer environments and data. | | | | | | | |
| **A1.1.1** | Logical separation is implemented as follows:<br>• The provider cannot access its customers' environments without authorization.<br>• Customers cannot access the provider's environment without authorization. | • Examine documentation.<br>• Examine system and network configurations.<br>• Interview responsible personnel. | ☒ | ☐ | ☐ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | | | | | |
| **A1.1.2** | Controls are implemented such that each customer only has permission to access its own cardholder data and CDE. | • Examine documentation.<br>• Examine system configurations. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **A1.1.3** | Controls are implemented such that each customer can only access resources allocated to them. | • Examine customer privileges. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |

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

| PCI DSS Requirement | | Expected Testing | Response ♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| **A1.1.4** | The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing. | • Examine the results from the most recent penetration test. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | The testing of adequate separation between customers in a multi-tenant service provider environment is in addition to the penetration tests specified in Requirement 11.4.6.<br>*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.* | | We do not store, process or transmit account data | | | | |
| **A1.2** Multi-tenant service providers facilitate logging and incident response for all customers. | | | | | | | |
| **A1.2.1** | Audit log capability is enabled for each customer's environment that is consistent with PCI DSS Requirement 10, including:<br>• Logs are enabled for common third-party applications.<br>• Logs are active by default.<br>• Logs are available for review only by the owning customer.<br>• Log locations are clearly communicated to the owning customer.<br>• Log data and availability is consistent with PCI DSS Requirement 10. | • Examine documentation.<br>• Examine system configuration settings. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit account data | | | | |
| **A1.2.2** | Processes or mechanisms are implemented to support and/or facilitate prompt forensic investigations in the event of a suspected or confirmed security incident for any customer. | • Examine documented procedures. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | | | We do not store, process or transmit 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 |
| **A1.2.3** | Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including:<br>• Customers can securely report security incidents and vulnerabilities to the provider.<br>• The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1. | • Examine documented procedures.<br>• Interview personnel. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | *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.* | | We do not store, process or transmit account data | | | | |

## *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** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | 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.<br>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. | | We do not store, process or transmit account data | | | | |

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

| PCI DSS Requirement | | Expected Testing | Response♦ (Check one response for each requirement) | | | | |
|---|---|---|---|---|---|---|---|
| | | | In Place | In Place with CCW | Not Applicable | Not Tested | Not in Place |
| **A2.1.2** | ***Additional requirement for service providers only:***<br>All service providers with existing connection points to POS POI terminals that use SSL and/or early TLS as defined in A2.1 have a formal Risk Mitigation and Migration Plan in place that includes:<br>• Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, and type of environment.<br>• Risk-assessment results and risk-reduction controls in place.<br>• Description of processes to monitor for new vulnerabilities associated with SSL/early TLS.<br>• Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments.<br>Overview of migration project plan to replace SSL/early TLS at a future date. | • Review the documented Risk Mitigation and Migration Plan. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a service provider. | | We do not store, process or transmit account data | | | | |
| **A2.1.3** | ***Additional requirement for service providers only***:<br>All service providers provide a secure service offering. | • Examine system configurations.<br>• Examine supporting documentation. | ☐ | ☐ | ☒ | ☐ | ☐ |
| | **Applicability Notes** | | *Describe results as instructed in "Requirement Responses" (page v)* | | | | |
| | This requirement applies only when the entity being assessed is a service provider. | | We do not store, process or transmit account data | | | | |

## *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.<br>***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 12.8.2 | We do not store, process or transmit account data |
| Requirement 12.9.2 | We do not store, process or transmit account data |
| Requirement 12.10 | We do not store, process or transmit account data |
| Requirement 3.7 | We do not store, process or transmit account data |
| Requirement 4 | We do not store, process or transmit account data |
| Requirement 5.2.3 | We do not store, process or transmit account data |
| Requirement 5.3.2.1 | We do not store, process or transmit account data |
| Requirement 5.3.3 | We do not store, process or transmit account data |
| Requirement 6.2 | We do not store, process or transmit account data |
| Requirement 6.3.2 | We do not store, process or transmit account data |
| Requirement 6.4.3 | We do not store, process or transmit account data |
| Requirement 12.8.1 | We do not store, process or transmit account data |
| Requirement 8.3.10 | We do not store, process or transmit account data |
| Requirement 8.3.11 | We do not store, process or transmit account data |
| Requirement 5.3.2.1 | We do not store, process or transmit account data |
| Requirement 9 | We do not store, process or transmit account data |
| Requirement 10 | We do not store, process or transmit account data |
| Requirement 11.2 | We do not store, process or transmit account data |
| Requirement 12.7 | We do not store, process or transmit account data |
| Requirement 3.4 | We do not store, process or transmit account data |
| Requirement A2 | We do not store, process or transmit account data |
| Requirement 8.2.3 | We do not store, process or transmit account data |
| Requirement 8.2.7 | We do not store, process or transmit account data |
| Requirement 8.3.9 | We do not store, process or transmit account data |
| Requirement 8.4.1 | We do not store, process or transmit account data |
| Requirement 12.3 | We do not store, process or transmit account data |
| Requirement 7 | We do not store, process or transmit account data |

| Requirement | Reason Requirement is Not Applicable |
|---|---|
| Requirement 3.5 | We do not store, process or transmit account data |
| Requirement 3.6 | We do not store, process or transmit account data |

## 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 the Requirement 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.* |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Section 3: Validation and Attestation Details

## Part 3. PCI DSS Validation

**This AOC is based on results noted in SAQ D (Section 2), dated (Self-assessment completion date** 26/01/2026***).***

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 entity identified in Part 2 of this document.

***Select one:***

| | |
|---|---|
| ☒ | **Compliant:** All sections of the PCI DSS SAQ are complete, and all assessed 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 Paritor Ltd 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 *(Service Provider Company Name)* has not demonstrated compliance with the PCI DSS requirements included in this SAQ.<br>**Target Date** for Compliance: *YYYY-MM-DD*<br>An entity 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 assessed 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 *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above or as Not in Place due to a legal restriction.<br>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 3. PCI DSS Validation *(continued)*

### Part 3a. Service Provider Acknowledgement

**Signatory(s) confirms:**

***(Select all that apply)***

| | |
|---|---|
| ☒ | *PCI DSS Self-Assessment Questionnaire D, Version 4.0.1,* was completed according to the instructions therein. |
| ☒ | All information within the above-referenced SAQ and in this attestation fairly represents the results of the entity's assessment in all material respects. |
| ☒ | PCI DSS controls will be maintained at all times, as applicable to the entity's environment. |

### Part 3b. Service Provider Attestation

| | |
|---|---|
| *Signature of Service Provider Executive Officer ↑* | *Date:* **23/01/2026** |
| *Service Provider Executive Officer Name:* **Simon Dutton** | *Title:* **Mr** |

### Part 3c. Qualified Security Assessor (QSA) Acknowledgement

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

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

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

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

| | |
|---|---|
| If an ISA(s) was involved or assisted with this assessment, indicate the role performed: | ☐ ISA(s) performed testing procedures. |
| | ☐ ISA(s) provided other assistance.<br>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 entity 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 systems and networks regularly | ☒ | ☐ | |
| 12 | Support information security with organizational policies and programs | ☒ | ☐ | |
| Appendix A1 | Additional PCI DSS Requirements for Multi-Tenant Service Providers | ☒ | ☐ | |
| Appendix A2 | Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections | ☒ | ☐ | |

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