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

Revision 3

Publication Date: August 2023

Document Changes

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

Contents

Document Changes i

Completing the Self-Assessment Questionnaire iii

Service Provider Eligibility Criteria for Self-Assessment Questionnaire D iii

Defining Account Data, Cardholder Data, and Sensitive Authentication Data iii

PCI DSS Self-Assessment Completion Steps iv

Expected Testing iv

Requirement Responses v

Additional PCI SSC Resources viii

Section 1: Assessment Information 1

Section 2a: Details about Reviewed Environment 8

Section 2b: Self-Assessment Questionnaire D for Service Providers 17

Build and Maintain a Secure Network and Systems 17

Requirement 1: Install and Maintain Network Security Controls 17

Requirement 2: Apply Secure Configurations to All System Components 23

Protect Account Data 28

Requirement 3: Protect Stored Account Data 28

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks 47

Maintain a Vulnerability Management Program 50

Requirement 5: Protect All Systems and Networks from Malicious Software 50

Requirement 6: Develop and Maintain Secure Systems and Software 54

Implement Strong Access Control Measures 65

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know 65

Requirement 8: Identify Users and Authenticate Access to System Components 70

Requirement 9: Restrict Physical Access to Cardholder Data 85

Regularly Monitor and Test Networks 97

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data 97

Requirement 11: Test Security of Systems and Networks Regularly 107

Maintain an Information Security Policy 122

Requirement 12: Support Information Security with Organizational Policies and Programs 122

Appendix A: Additional PCI DSS Requirements 141

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers 141

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections 144

Appendix A3: Designated Entities Supplemental Validation (DESV) 146

Appendix B: Compensating Controls Worksheet 147

Appendix C: Explanation of Requirements Noted as Not Applicable 148

Appendix D: Explanation of Requirements Noted as Not Tested 149

Section 3: Validation and Attestation Details 150

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 the cardholder data environment (CDE). Cardholder data and sensitive authentication data are considered account data and are defined as follows:

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

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

PCI DSS Self-Assessment Completion Steps

1. 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. All responses in this column also require completion of a Compensating Controls Worksheet (CCW) in Appendix B of this SAQ. Information on the use of compensating controls and guidance on how to complete the 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. 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. 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. Responses in this column may require the completion of Part 4, if requested by the entity to which this SAQ will be submitted. 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 new PCI DSS v4.0 requirement or bullet with an extended implementation period includes the following note: "*This requirement [or bullet] is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*"

These new requirements are not required to be included in a PCI DSS assessment until the future date has passed. Prior to that future date, any new requirements with an extended implementation date that have not been implemented by the 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 restriction is one where meeting the PCI DSS requirement would violate a local or regional law or regulation.*

Contractual obligations or legal advice are not legal restrictions.

Use of the Customized Approach

Use of the Customized Approach is not supported in SAQs.

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.

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

Additional PCI SSC Resources

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

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

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

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

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the 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:	Coralogix Ltd.
DBA (doing business as):	Coralogix
Company mailing address:	19 Abba Hillel Silver St., Ramat Gan
Company main website:	www.coralogix.com
Company contact name:	Shiran Wolfman
Company contact title:	Compliance Officer & DPO
Contact phone number:	+9720524739530
Contact e-mail address:	shiran@coralogix.com

Part 1b. Assessor	
Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not Applicable
Qualified Security Assessor	
Company name:	Not Applicable
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:	Coralogix	
Type of service(s) assessed:		
Hosting Provider: ☒ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web-hosting services ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Multi-Tenant Service Provider ☐ Other Hosting (specify):	**Managed Services:** ☐ Systems security services ☒ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POI / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ 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 □ Hardware □ Infrastructure / Network □ Physical space (co-location) □ Storage □ Web-hosting services □ Security services □ 3-D Secure Hosting Provider □ Multi-Tenant Service Provider □ Other Hosting (specify):	□ Systems security services □ IT support □ Physical security □ Terminal Management System □ Other services (specify):	□ POI / card present □ Internet / e-commerce □ MOTO / Call Center □ ATM □ 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):		

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.	Coralogix is an observability platform for customer logs, metrics, traces and security. Coralogix processes customer logs, which may include account data if the customers' systems are integrated this way. Coralogix provides tools to block/filter account data in logs before processing. Customer logs are stored on their own S3 buckets or obect storage buckets. Processing takes place within an AWS VPC in 1 of 5 geographically separate hosting regions (customers choice). Transmission of data is done securely with encryption in-transit utilizing TLS 1.3/1.2.

Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Coralogix operates on a secure infrastructure, implementing encryption protocols and access controls to safeguard sensitive information. Additionally, we continuously monitor and assess our systems for potential vulnerabilities, employing proactive measures to address any emerging threats promptly. Our commitment to security extends to regular third-party audits and assessments to ensure compliance with PCI DSS 4.0 requirements. Coralogix has the ability to positively impact the security of its customers' account data through the very nature of our services; to provide customers observability over their systems and/or applications through unique processing of logs, metrics, traces and security data.
Describe system components that could impact the security of account data.	Various system components collectively contribute to Coralogix's security infrastructure. The ability for processing systems employ encryption mechanisms, both in transit and at rest, to safeguard sensitive information from unauthorized access. Access controls and identity management systems are crucial components that regulate user permissions.

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	Cardholder logs are sent to our endpoint. Manipulation of data is done using our rule engine (logsparser). Data is saved for 12 hours in queuing. Data is passed and saved to our database for longer term (depends on the customer).
Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)*	☒ Yes ☐ No

Part 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*
Corporate office/headquarters	1	Ramat Gan, Israel
Affiliate Office (Coralogix Inc.)	1	Boston, MA, USA
Affiliate Office (Coralogix India Technology Services Pvt. Ltd.)	1	Bengaluru, India
Coralogix Germany GmbH	1	Franfurt, Germany
Data Centers (AWS)	7	Ireland (Dublin), Sweden (Stockholm), India (Mumbai), Singapore, US (East), US (West), US (GovCloud West)

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, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers

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:**
Stripe	Third-party payment processor
Amazon Web Services	IAAS/PAAS

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: Coralogix

PCI DSS Requirement	Requirement Responses *More than one response may be selected for a given requirement. Indicate all responses that apply.*				
	In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
Requirement 1:	☒	□	□	□	□
Requirement 2:	☒	□	□	□	□
Requirement 3:	☒	□	□	□	□
Requirement 4:	☒	□	□	□	□
Requirement 5:	☒	□	□	□	□
Requirement 6:	☒	□	□	□	□
Requirement 7:	☒	□	□	□	□
Requirement 8:	☒	□	□	□	□
Requirement 9:	☒	□	□	□	□
Requirement 10:	☒	□	□	□	□
Requirement 11:	☒	□	□	□	□
Requirement 12:	☒	□	□	□	□
Appendix A1:	☒	□	□	□	□
Appendix A2:	□	□	☒	□	□

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	Appendix A2: we are not using POS POI terminals.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	