Payment Card Industry

Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Matillion Ltd

Date of Report as noted in the Report on Compliance: 2026-09-18

Date Assessment Ended: 2026-08-31

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Section 1: Assessment Information

Instructions for Submission

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

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information

Part 1a. Assessed Entity (ROC Section 1.1)	
Company name:	Matillion Ltd
DBA (doing business as):	Matillion Ltd
Company mailing address:	Two New Bailey, Stanley Street, Salford, Manchester, Lancashire, United Kingdom, M3 5GS
Company main website:	www.matillion.com
Company contact name:	Mr. Graeme Park
Company contact title:	CISO
Contact phone number:	+44 1619388038
Contact e-mail address:	graeme.park@matillion.com

Part 1b. Assessor (ROC Section 1.1)	
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:	1 Cyber Valley Limited
Company mailing address:	128 City Road, London, United Kingdom, EC1V 2NX
Company website:	www.onecybervalley.com
Lead Assessor name:	Ms. Suhema Sashtikar
Assessor phone number:	+91 8983512628
Assessor e-mail address:	suhema@onecybervalley.com
Assessor certificate number:	PCI QSA - 207-249

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 2. Executive Summary

Part 2a. Scope Verification

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

Name of service(s) assessed:	Maia Foundation, a cloud-based data integration platform incorporating Maia, an AI-powered assistant designed to support customers in developing and managing data pipelines.

Type of service(s) 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): Maia Foundation is hosted on Amazon Web Services (AWS) cloud infrastructure, utilizing cloud-native applications and services

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.*

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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 Assessment (select all that apply):

Name of service(s) not assessed:	Not Applicable	
Type of service(s) not 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):		
Provide a brief explanation why any checked services were not included in the Assessment:	Not Applicable	

Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	Matillion provides Maia Foundation, a SaaS Agentic ETL / data-pipeline orchestration platform that allows customers to connect to, design, orchestrate, and execute pipelines against data sources and types of their own choosing — including, in some customer use cases, cardholder data that a customer elects to process through the platform. Matillion does not direct or restrict the categories of data customers choose to run through pipelines; card data handling is a function of customer choice and configuration, not a Matillion-initiated payment activity.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

	Separately, and unrelated to customer pipeline data, Matillion's own subscription billing is processed through AWS Marketplace and Azure Marketplace. Customers subscribe via their existing AWS or Azure accounts, with the marketplace provider handling cardholder data collection, authorization, and billing within its own environment; Matillion receives only account-level entitlement information confirming the subscription. For existing customers, Paystand, a PCI DSS-compliant third-party payment service provider, processes recurring billing transactions. Paystand stores and processes the associated cardholder data within its own environment; when customers update payment details, they are directed to a Paystand-hosted payment page, and Matillion does not directly handle the cardholder data submitted through this process
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Maia includes a data-sampling capability: the Maia AI agent, or a human user via the Designer UI, can request sample rows from a customer's data warehouse (accessed through a Runner deployed in the customer's environment, via the Component Information Service) to support pipeline development and AI-assisted actions. If a customer stores unencrypted cardholder data in their warehouse and directs Maia to query it, that data could transit Matillion's control plane via sampling results or Runner logs — noting this would also indicate the customer's own environment is not PCI DSS compliant independent of Matillion's platform. Matillion's position is that card data should never be used as raw pipeline input; the platform is not designed for that use case. Customer-facing controls over this exposure include: the ability to enable/disable Maia data sampling at the account level; the ability to accept or decline individual sampling requests during a Maia interaction; and the ability to disable Maia entirely, which disables sampling as well. Matillion advises customers to sample only from non-production environments, but does not technically enforce this. Sampled data and conversation state are encrypted at rest and, for conversation state, also at the application layer (double encryption); logs are stored in an encrypted Postgres database within Matillion's AWS account and are protected by SSL in transit.
Describe system components that could impact the security of account data.	The underlying AWS infrastructure supporting these systems could indirectly affect account data security if misconfigured.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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.*	Matillion's assessed environment covers two distinct paths: 1. Billing CDE: systems supporting subscription billing via AWS Marketplace and Azure Market entitlement and billing data flows into Matillion's internal systems for usage metering and invoicing, hosted across AWS VPCs with ALBs, PrivateLink, NAT Gateways, and Traefik for ingress/authentication. Wiz provides malware detection and configuration/threat monitoring. No cardholder data (PAN, expiration date, or cardholder name) is stored, processed, or transmitted by Matillion and can view only the last four digits of a card. 2. Maia data plane: where a customer independently elects to process cardholder data through a can transit the Designer UI, Maia Service, Component Information Service, Runner Gateway,and Runner, with sampled data and Runner logs reaching Matillion's control plane (encrypted, encrypted conversation-state database) and, for AI interactions, and LangFuse. This path is customer-initiated and customer-scoped. Matillion does not design for or solicit cardholder data as pipeline input.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☐ Yes ☒ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this 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	3	Manchester Denver Hyderabad
Data Centre	1	USA

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

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
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
				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.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers (ROC Section 4.4)

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 entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, 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 Services Provided:
AWS	Cloud Hosting Provider
Paystand	Payment Processing Services

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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

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: Maia Foundation, a cloud-based data integration platform incorporating Maia, an AI-powered assistant designed to support customers in developing and managing data pipelines.

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.2.6 - There are no insecure services enabled. 1.3.3 - There is no wireless network in scope. 1.4.4 - Matillion do not store CHD in their environment. 2.2.5 - No insecure service are running in Matillion enviornment. 2.3.1, 2.3.2 - There is no wireless network in scope. Requirement 3 - Matillion do not store CHD in their environment. Requirement 4- Matillion does not transmit any cardholder data over public networks. 5.2.3, 5.2.3.1 - There are no system components in scope which are not at risk for malware. 5.3.3 - There is no removable electronic media in scope. 6.4.1 - This requirement is superseded by the requirement 6.4.2. 7.2.6 - Matillion do not store CHD in the environment. 8.2.2 - Matillion do not use group, shared or generic accounts. 8.2.3 - Matillion do not have remote access to their customer premises. 8.3.9 - There is no single factor authentication used in Matillion. 8.3.10, 8.3.10.1 - No customer user has access to Matillion environment. 8.6.1, 8.6.2 - No accounts have been used for interactive login. 9.4 - No physical media in scope. 9.5 - No POI devices are in scope. 10.7.1 - This requirement is superseded by requirement 10.7.2. 11.2.1, 11.2.2 - There is no wireless network in scope. 11.4.2 - There is no internal IPs in scope. 11.4.5, 11.4.6 - No segmentation is used in scope. 12.3.2 - There is no customised approach used. Appendix A2 - No POI terminals are in scope.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	None

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2026-07-06
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2026-08-31
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ No

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC 2026-09-18)*.

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

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC 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 ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby (Matillion Ltd) has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC 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 PCI DSS requirements. **Target Date** for Compliance: *YYYY-MM-DD* 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 ROC 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 In Place or 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 except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

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

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the 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

Graeme Park
Graeme Park (Oct 6, 2026 12:22:54 GMT+1)

Signature of Service Provider Executive Officer ↗	Date: 2026-09-18
Service Provider Executive Officer Name: Mr. Graeme Park	Title: CISO

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

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

Signature of Lead QSA ↗	Date: 2026-09-18
Lead QSA Name: Ms. Suhema Sashtikar	

Signature of Duly Authorized Officer of QSA Company ↗	Date: 2026-09-18
Duly Authorized Officer Name: Mr. Parminder Lall	QSA Company: 1 Cyber Valley Limited

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

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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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 Non-Compliant results 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 provide 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 their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.