

Payment Card Industry Data Security Standard

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

For use with PCI DSS Version 4.0.1

Revision 1

Publication Date: December 2024

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.

This AOC reflects the results documented in an associated Self-Assessment Questionnaire (SAQ).

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Self-Assessment Questionnaire.

Part 1. Contact Information

Part 1a. Assessed Entity

Company name:	Meadow AI
DBA (doing business as):	Not Applicable
Company mailing address:	1107 23rd Ave E, Seattle WA 98112
Company main website:	meadow.ai
Company contact name:	Abbas Guvenilir
Company contact title:	Chief Operations Officer
Contact phone number:	8454532016
Contact e-mail address:	abbas@meadow.ai

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:	Insight Assurance LLC
Company mailing address:	400 N. Tampa St. 15th Floor - Suite 129 Tampa, FL 33602
Company website:	https://insightassurance.com
Lead Assessor Name:	Deon Ladson
Assessor phone number:	843-312-4043
Assessor e-mail address:	deon@insightassurance.com
Assessor certificate number:	QSA 206-828

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:

Network Infrastructure and Surveillance Camera Service

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):
Network Services

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): Not Applicable

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: 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

Describe how the business stores, processes, and/or transmits account data.

Meadow is a service provider offering managed network infrastructure and surveillance camera solutions (CCTV/NVR) for merchants across the United States. Their mission is to support secure and efficient retail operations by delivering robust connectivity and visual monitoring systems, especially in environments where payment transactions occur.

As a Service Provider, Meadow supports multiple merchants with their network and surveillance setup. While Meadow does not store, process, or transmit cardholder data directly, their managed network devices may handle encrypted cardholder data in transit, such as when a merchant's POS system communicates with third-party payment gateways.

Meadow does not directly handle card-present transactions. However, in cases where Meadow

	provides networking infrastructure or surveillance solutions to merchants (e.g., restaurants), those merchants may operate POS terminals that process in-person payments. In such cases, card-present transactions occur within the merchant environment, and any card data transmission is managed by the merchant's payment solution, not Meadow.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Not Applicable
Describe system components that could impact the security of account data.	Not Applicable

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.*

Meadow has deployed a network infrastructure and surveillance system at various merchant sites (restaurants) to facilitate connectivity and security. This environment enables the merchant's Point-of-Sale (POS) devices to connect to the internet for payment processing.

Key Components

Network Equipment: The core network components include:

Ubiquiti routers and access points (APs) for wireless connectivity and routing.

Netgear and Mokerlink switches for network segmentation and connectivity.

Location: All network devices are physically located at the merchant sites.

Connectivity: This system provides the necessary connection for POS devices to communicate with external payment networks (e.g., through the internet).

Surveillance: The environment also includes a monitoring system comprised of IP cameras connected to the same network infrastructure.

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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Not applicable	Not applicable	Not applicable

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)
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable

- * 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:
Not Applicable	Not Applicable

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: Network Infrastructure and Surveillance Camera Service

PCI DSS Requirement	Requirement Responses				
	<i>More than one response may be selected for a given requirement. Indicate all responses that apply.</i>				
	In Place	In Place with CCW	Not Applicable	Not 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.	1.5 - Meadow does not have CDE, hence this requirement is not applicable. R3 - Meadow does not store, process, transmit card holder data, hence, this requirement is not applicable. R4 - Meadow does not store, process, transmit card holder data, hence, this requirement is not applicable. 5.2, 5.3 - There is no in-scope server, hence this requirement is not applicable. 6.2, 6.3.2, 6.4, 6.5.3, 6.5.4, 6.5.5, 6.5.6 - Meadow does not have any in-scope applications, hence, this requirement is not applicable. 6.4.1 - Requirement Superseded. 8.3.10 - Requirement Superseded. 8.3.11 - Customer is not allowed to access the Meadow's network devices. Hence this requirement is not applicable. 8.2.3 - Meadow does not remotely access to customer's system, hence this requirement is not applicable. 8.5, 8.4, 8.6 - Meadow does not have in-scope system, hence this requirement is not applicable. 9.3 - The merchant locations are managed by them, hence, visitor management is not applicable to Meadow. 9.4 - Meadow does not store the card holder data, hence this requirement is not applicable. 9.5 - POI is managed by the merchant, hence this requirement is not applicable. 10.7.1 - Requirement Superseded. 11.3.2, 11.3.2.1 - There is no in-scope public ip, hence this requirement is not applicable. 11.4.5 - There is no CDE, hence, this requirement is not applicable. 11.4.7 - Meadow is not a multi-tenant service provider, hence this requirement is not applicable. 11.5 - There is no CDE in Meadow environment. Hence this requirement is not applicable. 11.6 - Meadow does not have payment page, hence this requirement is not applicable. 12.3 - Meadow does not handled the card holder data, hence this requirement is not applicable. 12.10.7 - Meadow does not store PAN, hence this requirement is not applicable. A1 - Meadow is not a multi-tenant service provider, hence this requirement is not applicable. A2 - Meadow does not manage POS, hence this requirement is not applicable
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	2025-10-30
Were any requirements in the SAQ unable to be met due to a legal constraint?	☐ Yes ☒ No

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 2025-10-30).

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 (<i>Meadow AI</i>) 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 (<i>Service Provider Company Name</i>) has not demonstrated compliance with the PCI DSS requirements included in this SAQ. 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 <i>before completing Part 4</i>.								
☐	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 (<i>Service Provider Company Name</i>) 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. This option requires additional review from the entity to which this AOC will be submitted. <i>If selected, complete the following:</i> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								

Part 3a. 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

Abbas Guvenilir

Signature of Service Provider Executive Officer ↑	Date: 2025-10-30
Service Provider Executive Officer Name: Abbas Guvenilir	Title: Chief Operations Officer

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: *SAQ-D/AOC Review.*

Deon Ladson

Signature of Lead QSA ↑	Date: 2025-10-30
Lead QSA Name: Deon Ladson	

Aaron Getchius

Signature of Duly Authorized Officer of QSA Company ↑	Date: 2025-10-30
Duly Authorized Officer Name: Aaron Getchius	QSA Company: Insight Assurance LLC

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

If an ISA(s) was involved or assisted with this assessment, indicate the role performed:

☐ ISA(s) performed testing procedures.

☐ ISA(s) provided other assistance.

If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

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

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the 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/.

CERTIFICATE *of* SIGNATURE

REF. NUMBER
KM2X7-INOVG-BSGX6-XC5EJ

DOCUMENT COMPLETED BY ALL PARTIES ON
24 OCT 2025 06:15:33
UTC

SIGNER

AARON GETCHIUS

EMAIL
AARON@INSIGHTASSURANCE.COM

TIMESTAMP

SENT
21 OCT 2025 19:29:58

VIEWED
21 OCT 2025 20:18:19

SIGNED
21 OCT 2025 20:18:33

SIGNATURE

Aaron Getchius

IP ADDRESS
104.5.136.137

LOCATION
COMBINED LOCKS, UNITED STATES

RECIPIENT VERIFICATION

EMAIL VERIFIED
21 OCT 2025 20:18:19

DEON LADSON

EMAIL
DEON@INSIGHTASSURANCE.COM

SENT
21 OCT 2025 19:29:58

VIEWED
21 OCT 2025 22:40:59

SIGNED
21 OCT 2025 22:41:17

Deon Ladson

IP ADDRESS
47.201.246.194

LOCATION
DAVENPORT, UNITED STATES

RECIPIENT VERIFICATION

EMAIL VERIFIED
21 OCT 2025 22:40:59



CERTIFICATE *of* SIGNATURE

REF. NUMBER
KM2X7-INOVG-BSGX6-XC5EJ

DOCUMENT COMPLETED BY ALL PARTIES ON
24 OCT 2025 06:15:33
UTC

SIGNER

ABBAS GUVENILIR

EMAIL
ABBAS@MEADOW.AI

TIMESTAMP

SENT
21 OCT 2025 19:29:58

VIEWED
24 OCT 2025 06:13:53

SIGNED
24 OCT 2025 06:15:33

SIGNATURE

Abbas Guvenilir

IP ADDRESS
174.21.177.129

LOCATION
SEATTLE, UNITED STATES

RECIPIENT VERIFICATION

EMAIL VERIFIED
24 OCT 2025 06:13:53

