



A-LIGN

Cloud Software Group, Inc.

Payment Card Industry (PCI)
Data Security Standard

2024 Attestation of Compliance





Payment Card Industry Data Security Standard

Attestation of Compliance for Report on Compliance - Service Providers

Version 4.0

Revision 2

Publication Date: August 2023

PCI DSS v4.0 Attestation of Compliance for Report on Compliance - Service Providers

Entity Name: Cloud Software Group, Inc.

Assessment End Date: 28 October 2024

Date of Report as noted in the Report on Compliance: 9 November 2024

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:	Cloud Software Group (CSG)
DBA (doing business as):	Not Applicable.
Company mailing address:	851 W. Cypress Creek Rd., Fort Lauderdale, Florida 33309 USA
Company main website:	https://www.cloud.com
Company contact name:	Mustafa Kagalwala
Company contact title:	GRC Director
Contact phone number:	+1 (800) 242-8749
Contact e-mail address:	mustafa.kagalwala@cloud.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:	A-LIGN Compliance and Security, Inc. dba A-LIGN
Company mailing address:	400 N. Ashley Drive, Suite 1325, Tampa, Florida 33602 USA
Company website:	https://www.A-LIGN.com
Lead Assessor name:	Daniel Powers
Assessor phone number:	+1 (888) 702-5446
Assessor e-mail address:	Daniel.powers@A-LIGN.com

Assessor certificate number: 203-707

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: CSG Citrix DaaS

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 Assessment (select all that apply):

Name of service(s) not assessed:	ActiveMatrix BPM, ActiveSpaces, BusinessConnect, BusinessEvents, BusinessWorks, Cloud AuditSafe, Cloud Events, Cloud Services Systems, Cloud Integration, Cloud Live Apps, Cloud Messaging, Cloud Tropos, Data Science, Data Virtualization, EBX, eFTL, Enterprise Message Service, Flogo Enterprise, Foresight, FTL, Graph Database, GridServer, Jaspersoft, Live Datamart, LogLogic, Managed File Transfer, MDM, Messaging, Messaging - Apache Kafka Distribution, Messaging - Eclipse Mosquitto Distribution, Nimbus, Rendezvous, Reward, Spotfire, StreamBase
----------------------------------	---

Type of service(s) not assessed:

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

Provide a brief explanation why any checked services were not included in the Assessment:

Services were confirmed to be segmented from the Citrix DaaS environment and would be assessed separately from Citrix DaaS (SaaS) environment.

Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

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

CSG's Citrix DaaS environment does not directly store, process, and/or transmit cardholder data, however

	these systems support customer APIs that may be used for this purpose.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	<p>The CSG Citrix Desktop as a Service (formerly known Citrix Virtual Application and Desktop Service) offers secure access to virtual Windows, Linux, web applications, and desktops. This service is based on Desktop as a Service technology. Available as a cloud service or hybrid solution, it allows customers to choose the deployment option that best aligns with their enterprise cloud.</p> <p>Desktop as a Service is a virtualization solution that enables universal access to virtual applications, desktops, and data with the option to implement a scalable virtual desktop infrastructure (VDI) solution. Desktop as a Service enables:</p> <ul style="list-style-type: none"> • End users to run applications and desktops independently of the device's operating system and interface • Administrators to manage the network and provide or restrict access from selected devices or from all devices • Administrators to manage an entire network from a single data center
Describe system components that could impact the security of account data.	Citrix DaaS is a cloud-hosted solution managed by Cloud Software Group. Cloud services include virtualized compute, networking, and storage to provide the Citrix DaaS software as a service solution.

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.*

The assessed environment consisted of multiple networks hosted within a PCI compliant cloud service provider. Each network contained connections into and out of the CDE.

Critical system components include the following:

- Azure Virtual Private Networks (VNet)
- Azure Network Security Controls
- Azure services
- Administrative Workstations

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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Azure - Cloud Data Center	Undisclosed	Undisclosed

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.

[♦] 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 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)) | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> 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) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| • Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers). | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |

If Yes:

Name of Service Provider:	Description of Services Provided:
Microsoft Azure	Cloud Services Provider
Okta	SSO Services
Google Security Operations	SIEM Services

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

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: CSG Citrix DaaS

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
Requirement 1:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.

Requirement 1.2.4; 1.4.4; 3.1.1-3.7.9; 4.1.1-4.2.2; 7.2.6; 12.3.3 - Not Applicable. The assessor verified through interviews with responsible personnel and review of policy and procedure documentation that CSG Citrix DaaS does not directly store, process, and/or transmit cardholder data. Customers using the Citrix DaaS service may store, process, or transmit cardholder, although compliance with this requirement is their responsibility.

Requirement 1.2.6; 2.2.5 - Not Applicable. The assessor verified that no insecure services, protocols, and ports were in use.

Requirement 1.3.3; 2.3.1; 2.3.2 - Not Applicable. CSG Citrix DaaS' environment is hosted within a controlled cloud environment where wireless networks are explicitly prohibited.

Requirement 1.4.5 - Not Applicable. The assessor examined NSC configurations and interviewed CSG Citrix DaaS personnel who explained the disclosure of private IP addresses is not permitted.

Requirement 5.2.3.1; 5.3.2.1; 5.4.1; 6.3.2; 6.4.2; 7.2.4; 7.2.5; 7.2.5.1; 8.3.6; 8.3.10; 8.3.10.1; 8.5.1; 11.3.1.1; 11.3.1.2; 11.5.1.1; 12.3.1; 12.3.4; 12.5.2.1; 12.5.3; 12.6.2; 12.6.3.1; 12.6.3.2; 12.10.4.1; 12.10.7; A1.1.4 - Not Applicable. This requirement is a best practice until 31 March 2025.

Requirement 5.3.3 - Not Applicable. CSG Citrix DaaS' environment is hosted within a controlled cloud environment where removable electronic media is explicitly prohibited.

Requirement 6.4.3; 11.6.1 - Not Applicable. The assessor reviewed the network diagram, data flow and related business processes, interviewed relevant personnel, and verified that CSG does not manage or provide any payment pages.

Requirement 6.5.2; 11.3.1.3; 11.3.2.1 - Not Applicable. The assessor verified there were no significant changes by interviewing CSG Citrix DaaS stakeholders regarding the status of the entity's in-scope systems and networks for the past 12 months. In addition, the assessor reviewed change management records, network diagrams, cardholder data flow diagrams, and business workflows to confirm there were no significant changes during the time period being assessed.

Requirement 6.5.5 - Not Applicable. The assessor interviewed CSG Staff and observed development processes to confirm neither PAN nor CHD is required or utilized for software development.

Requirement 8.2.2 - Not Applicable. The assessor interviewed CSG Citrix DaaS' stakeholders and examined users with access to the production environment in AWS to confirm group, shared, generic accounts and shared authentication credentials are not utilized.

Requirement 8.2.3 - Not Applicable. The assessor reviewed the network diagram, the cardholder business workflow and related business processes,

	<p>interviewed relevant personnel, and verified that CSG Citrix DaaS does not maintain access to their customer's premises.</p> <p>Requirement 8.2.7 - Not Applicable. Based on a review of the user listing of in-scope system components, the network diagram, interviews with relevant personnel, the assessor verified that the entity does not allow third-party access into the CDE or in-scope environment.</p> <p>Requirement 8.3.9 - Not Applicable. The assessor verified that all authentication into in-scope systems required MFA.</p> <p>Requirement 8.6.1-8.6.3 - Not Applicable. The assessor reviewed the authentication flow and configuration, user listing, access management policies and interviewed relevant personnel and verified that interactive login is not possible or permitted within the in-scope environment.</p> <p>Requirement 9.4.1-9.4.7 - Not Applicable. The assessor reviewed the data flow diagram, data retention and management processes, business processes involving cardholder data, interviewed relevant personnel, and verified that no media was utilized for transmitting, storing, or processing cardholder data.</p> <p>Requirement 9.5.1-9.5.1.3 - Not Applicable. The assessor reviewed the data flow diagram, business processes, interviewed relevant personnel to confirm CSG Citrix DaaS does not utilize POI devices in part of the services assessed.</p> <p>Requirement 10.4.2.1 - Not Applicable. The assessor reviewed the audit logging processes, the internal logging system, the security logging policies and procedures and interviewed relevant personnel to confirm that all audit logs are analyzed by an automated mechanism, including logs from all systems not specified in Requirement 10.4.1.</p> <p>Requirement 11.4.4 - Not Applicable. Based on the references listed below, the assessor verified there were no exploitable vulnerabilities or security weaknesses found during the internal and external penetration testing performed.</p> <p>Requirement 12.3.2 - Not Applicable. CSG Citrix DaaS does not use a customized approach for any applicable PCI requirements.</p> <p>Requirement A2.1.1-A2.1.3 - Not Applicable. The entity does not utilize POS/POI terminals.</p>
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable.

Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3.2)

Date Assessment began: Note: This is the first date that evidence was gathered, or observations were made.		22 July 2024
Date Assessment ended: Note: This is the last date that evidence was gathered, or observations were made.		28 October 2024
Were any requirements in the ROC unable to be met due to a legal constraint?		<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed:		<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Examine documentation	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Interview personnel	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Examine/observe live data	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Observe process being performed	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Observe physical environment	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
• Interactive testing	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
• Other: Not Applicable.	<input type="checkbox"/> Yes	<input type="checkbox"/> No

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 9 November 2024.

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*):

<input checked="" type="checkbox"/>	<p>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 Cloud Software Group, Inc. has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p>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.</p> <p>Target Date for Compliance:</p> <p>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.</p>								
<input type="checkbox"/>	<p>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.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <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 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Kumar Palaniappan

Signature of Service Provider Executive Officer ↑	Date: 12 November 2024
Service Provider Executive Officer Name: Kumar Palaniappan	Title: VP, Product Security

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:

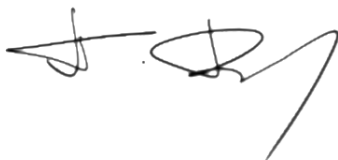
☒ QSA performed testing procedures.

☐ QSA provided other assistance.

If selected, describe all role(s) performed: Not Applicable.



Signature of Lead QSA ↑	Date: 9 November 2024
Lead QSA Name: Daniel Powers	



Signature of Duly Authorized Officer of QSA Company ↑	Date: 12 November 2024
Duly Authorized Officer Name: Petar Besalev, EVP Cybersecurity and Compliance Services	QSA Company: A-LIGN

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 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input type="checkbox"/>	<input type="checkbox"/>	

