Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance

Prepared for:

Cloud Software Group, Inc.

Date:

28 February 2025

A-LIGN

A-LIGN.COM

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: Cloud Software Group, Inc.

Date of Report as noted in the Report on Compliance: 28 February 2025

Date Assessment Ended: 28 February 2025

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, Inc.
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:	Sr. Manager - Risk Management
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:	Tim Cunningham
Assessor phone number:	+1 (888) 702-5446
Assessor e-mail address:	Timothy.Cunningham@A-LIGN.com
Assessor certificate number:	QSA, 201-323

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

Provide a brief explanation why any checked services were not included in the Assessment:	Services were confirmed to be segmented from the Citrix Gateway Service environment and are assessed separately from the Citrix Gateway Service (SaaS) environment.

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.	Citrix Gateway Service does not directly store, process or transmit CHD but provides a platform through which client-managed CHD could flow.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	The service under assessment is an element of the Citrix Cloud Platform. The Citrix Gateway Service is a key component of the Citrix Cloud Platform that provides Enterprise users secure access to their Virtual Apps and Desktops. It is a globally distributed multi-tenant service hosted and managed by Citrix. The following services or functions have been excluded from the scope of this assessment: 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 Mosquito Distribution, Nimbus, Rendezvous, Reward, Spotfire, StreamBase.
Describe system components that could impact the security of account data.	The system components that could impact the security of account data include the AWS and Azure cloud management consoles, which manage virtualized computing resources and storage. The Amazon VPC and Azure VNet provide segmented workspaces and ensure secure network connectivity. AWS IAM, MS Entra and Okta SSO are used for secure single sign-on and identity management. Virtualized computing resources are provided by AWS EC2 and Azure VM instances. Administrator workstations are used for production access. Microsoft Defender and AWS GuardDuty are employed for threat detection and response. Additionally, Splunk is utilized for logging activities.

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.*	The assessed environment consisted of a designated VPC hosted within a PCI compliant cloud service provider. The VPC was connected to other VPCs in the Citrix suite of services providing Enterprise users secure access to their Virtual Apps and Desktops. Critical system components include load balancers, Security Groups and Virtual machines.

• *System components that could impact the security of account data.*	System components that could impact the security of account data include IDS/IPS systems, anti-malware systems and log correlation systems. Network security enforcement includes Security Groups provided by the Cloud Hosting provider and configured by the assessed entity.
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)
Cloud Hosting Provider - AWS	Multiple Points of Presence	Global
Cloud Hosting Provider - Azure	Multiple Points of Presence	Global
Corporate HQ	1	Ft Lauderdale, FL, USA

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, 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
*(***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:**
Amazon Web Services	On-demand cloud computing platform that hosts the entity application/services
Microsoft Azure	On-demand cloud computing platform that hosts the entity application/services
Okta	Single Sign-On (SSO) Platform to access the environment.
Splunk	Splunk Cloud Services - SIEM audit log correlation

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: Citrix Gateway Service

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

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.2.6: Not Applicable. No insecure services, daemons, or protocols were identified. 1.3.3: Not Applicable. No wireless networks connecting to the CDE or transmitting CHD are present. 1.4.5: Not Applicable. The entity does not disclose private IP addresses. 2.2.5: Not Applicable. No insecure services, daemons, or protocols were identified. 2.3.1 - 2.3.2: Not Applicable. No wireless networks connecting to the CDE or transmitting CHD are present. 3.1.1 - 3.7.9: Not Applicable. The entity does not directly store, process, and/or transmit CHD. 4.1.1 - 4.2.2: Not Applicable. The entity does not directly store, process, and/or transmit CHD. 5.2.3.1: Not Applicable. This requirement is a best practice until 31 March 2025. 5.3.2.1: Not Applicable. This requirement is a best practice until 31 March 2025. 5.3.3: Not Applicable. Removable electronic media ports are disabled on all endpoints. 5.4.1: Not Applicable. This requirement is a best practice until 31 March 2025. 6.4.3: Not Applicable. This requirement is a best practice until 31 March 2025. 6.5.2: Not Applicable. No significant changes have occurred in the past 12 months. 7.2.4 - 7.2.5.1: Not Applicable. This requirement is a best practice until 31 March 2025. 7.2.6: Not Applicable. The entity does not directly store, process, and/or transmit CHD. 8.2.2: Not Applicable. No group, generic or other shared accounts were present on any in-scope system component. 8.2.3: Not Applicable. The entity does not access customer premises. 8.2.7: Not Applicable. Third-party access is not allowed. 8.3.6: Not Applicable. This requirement is a best practice until 31 March 2025. 8.3.9 - 8.3.10: Not Applicable. All authentication into in-scope systems required MFA. 8.5.1 - 8.6.3: Not Applicable. This requirement is a best practice until 31 March 2025. 9.5.1 - 9.5.1.3: Not Applicable. The entity does not use POS/POI within the environment. 10.4.1.1: Not Applicable. This requirement is a best practice until 31 March 2025. 10.4.2.1: Not Applicable. This requirement is a best practice until 31 March 2025. 10.7.2: Not Applicable. This requirement is a best practice until 31 March 2025. 11.3.1.1 - 11.3.1.2: Not Applicable. This requirement is a best practice until 31 March 2025.

	11.3.1.3: Not Applicable. No significant changes have occurred in the past 12 months. 11.3.2.1: Not Applicable. No significant changes have occurred in the past 12 months. 11.4.5, 11.4.6: Not Applicable. No segmentation is used to isolate the CDE from other networks. 11.4.7: Not Applicable. This requirement is a best practice until 31 March 2025. 11.5.1.1: Not Applicable. This requirement is a best practice until 31 March 2025. 12.3.1 - 12.3.4: Not Applicable. This requirement is a best practice until 31 March 2025. 12.5.2.1 - 12.5.3: Not Applicable. This requirement is a best practice until 31 March 2025. 12.6.2: Not Applicable. This requirement is a best practice until 31 March 2025. 12.6.3.1 - 12.6.3.2: Not Applicable. This requirement is a best practice until 31 March 2025. 12.10.4.1: Not Applicable. This requirement is a best practice until 31 March 2025. 12.10.7: Not Applicable. This requirement is a best practice until 31 March 2025. A1.1.4: Not Applicable. This requirement is a best practice until 31 March 2025. A2.1.1 - A2.1.3: Not Applicable. The entity does not utilize POS/POI within the environment.
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**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	01 December 2024
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	28 February 2025
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

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 28 February 2025.

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 **Cloud Software Group, Inc.** 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: 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

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

Kumar Palaniappan

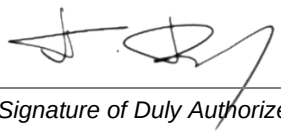
Signature of Service Provider Executive Officer ↗	Date: 28 February 2025
Service Provider Executive Officer Name: Kumar Palaniappan	Title: VP, CISO

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: Not Applicable.

T J Cunningham

Signature of Lead QSA ↗	Date: 28 February 2025
Lead QSA Name: Tim Cunningham	



Signature of Duly Authorized Officer of QSA Company ↗	Date: 28 February 2025
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	☐	☐	
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/