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

Date of Report as noted in the Report on Compliance: November 17, 2025

Date Assessment Ended: October 31, 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
DBA (doing business as):	Not applicable.
Company mailing address:	851 W. Cypress Creek Road, Fort Lauderdale, FL 33309
Company main website:	https://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:	Schellman Compliance, LLC
Company mailing address:	4010 W Boy Scout Boulevard, Suite 600, Tampa, FL 33607
Company website:	https://www.schellman.com/services/pci-compliance
Lead Assessor name:	Ryan Renner
Assessor phone number:	866.254.0000
Assessor e-mail address:	pcirocs@schellman.com
Assessor certificate number:	QSA Certificate # 205-016

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 Application Delivery Management (ADM), Citrix Desktop as a Service (CDS), and Citrix Endpoint Management (CEM)

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):
Not applicable.

Managed Services:

☐ Systems security services
☐ IT support
☐ Physical security
☐ Terminal Management System
☐ Other services (specify):
Not applicable.

Payment Processing:

☐ POI / card present
☐ Internet / e-commerce
☐ MOTO / Call Center
☐ ATM
☐ Other processing (specify):
Not applicable.

☐ 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 Assessment (select all that apply):

Name of service(s) not assessed:	All other CSG services.	
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): Not applicable.	**Managed Services:** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify): Not applicable.	**Payment Processing:** ☐ POI / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify): Not applicable.
☐ 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.		
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.	Cloud Software Group's (CSG) CDS, CEM, and ADM environments do not directly transmit, store or process cardholder data. CSG only provided cloud and virtualization technologies that customers used for their instances which may have cardholder data present.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Administrators who manage the in scope environments can impact security by setting access controls, using secure tooling and development methods for the underlying software, and configuring network boundaries. Misconfigurations can expose customer data to unauthorized access and centralized

	management can potentially increase the impact of any configuration errors or insider threats.
Describe system components that could impact the security of account data.	ActiveMatrix BPM (Business Process Management), 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

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 Cloud Software Group (CSG) Citrix Cloud Platform serves as a centralized hub for hosting and managing Citrix cloud services. The services include Desktop as a service, Citrix Endpoint Management, and Application Delivery Management. The platform integrates with customer resources by utilizing connectors that operate across a diverse range of environments, including on-premises infrastructure, public cloud, private cloud, or hybrid cloud implementations. Customers create, oversee, and deploy workspaces where they may be storing, processing or transmitting cardholder data at their own discretion and only for their business needs. CSG's environments do not directly handle cardholder data.
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)
Corporate Headquarters	One (1)	One (1)
Amazon Web Services (AWS)	Six (6)	ap-south ap-southeast eu-central eu-west us-west us-east
Microsoft Azure	16	australiaeast australiasoutheast eastus eastus2 global japaneast japanwest northcentralus northeurope southcentralus southeastasia

		uksouth westeurope westus westus2 westus3

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.

[♦] For purposes of this document, ”Lists of Validated Products and Solutions” means the lists of validated products, solutions, and/or components appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers
*(***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	Hosting provider
Azure	Hosting provider
Okta	Identity and Authentication
Google	Security incident event management systems
Akamai	Web Application Firewall
Splunk	Log collection and aggregation
Grafana	Log collection and aggregation

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 Application Delivery Management (ADM), Citrix Desktop as a Service (CDS), and Citrix Endpoint Management (CEM)

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:	☐	☒	☐	☐	☐
Appendix A3:	☐	☒	☐	☐	☐

Justification for Approach

Part 2. Executive Summary *(continued)*

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.3.3, 2.3.1, 2.3.2: There were no wireless networks within or connected to the in-scope environment. 1.4.4, 3.1.1 – 3.7.9, 4.1.1 – 4.2.2, 6.5.5, 7.2.6: CHD was not directly stored, processed or transmitted. CSG's customers were responsible for meeting this requirement. 6.4.1, 8.3.10, 10.7.1: This requirement has been superseded as of March 31, 2025. 6.4.3, 11.6.1: CSG did not have any payment pages within the in-scope environment. 8.2.3: CSG did not have remote access to customer premises 9.4.1 – 9.4.7: CSG did not maintain any hard-copy or electronic media that contained cardholder data. 9.5.1 – 9.5.1.3, A2.1.1 – A2.1.3: CSG did not maintain any POI devices. CSG customers were responsible for complying with this requirement. 11.3.1.3, 11.3.2.1: No significant changes occurred to the in-scope environment during the previous 12 months. 12.3.2: The customized approach was not utilized to fulfill any requirements in this assessment. 12.5.3: No significant changes to CSG's organizational structure occurred during the previous 12 months.
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.*	July 13, 2025
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	October 31, 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 *November 17, 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* 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 *Cloud Software Group* has not demonstrated compliance with PCI DSS requirements.

Target Date for Compliance: Not applicable.

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 *Cloud Software Group* 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: 11/21/2025
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.

Signed by:
Ryan Renner
A8CE9BA47528442...

Signature of Lead QSA ↑	Date: 11/22/2025
Lead QSA Name: Ryan Renner	

DocuSigned by:
Matt Crane
AA964E80BBB646D...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 11/21/2025
Duly Authorized Officer Name: Matt Crane	QSA Company: Schellman Compliance, 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: Not applicable.

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

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/