



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022



Document Changes

Date	Version	Description
September 2022	3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.



Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

Company Name:	Cloud Software Group, Inc.		DBA (doing business as):			
Contact Name:	Meghan Hester		Title:	Senior Director of IT Governance and Business Operations		
Telephone:	800-242-8749		E-mail:	meghan.hester@cloud.com		
Business Address:	851 W Cypress Creed Rd, Fort Lauderdale, FL 33309		City:	Fort Lauderdale		
State/Province:	FL	Country:	USA		Zip:	33309
URL:	https://cloud.com					

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	risk3sixty, LLC				
Lead QSA Contact Name:	Jeremy Brandt	Title:	Senior Associate		
Telephone:	404-717-2778	E-mail:	jeremy.brandt@risk3sixty.com		
Business Address:	408 S Atlanta St, Suite 180	City:	Roswell		
State/Province:	GA	Country:	30075	Zip:	30075
URL:	https://risk3sixty.com				



Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:		NetScaler Application Delivery Management (ADM)	
Type of service(s) 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 <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	Managed Services (specify): <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"/> POS / 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 checked="" type="checkbox"/> Others (specify): Web based micro services (ADP, CMP, Front End, and Monitoring) via an agent that is onboarded on Amazon Web Services' hosted environment or on customer premises that simplify application delivery infrastructure			

Note: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.


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 (check all that apply):

Name of service(s) not assessed: Netscaler ADC VPX Gateway, hardware models, and all other microservices for ADM outside of ADP, CMP, Front End and Monitoring

Type of service(s) not assessed:

Hosting Provider:

- ☒ Applications / software
- ☒ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Shared Hosting Provider
- ☐ Other Hosting (specify):

Managed Services (specify):

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

Payment Processing:

- ☐ POS / 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:

Risk3sixty set scope boundaries, with agreement from ADM's SRE team, around the ADP, CMP, Front End, and Monitoring microservices, bastion hosts, as well as supporting shared services to test PCI controls against, since they are 'security impacting' system components for customer environments, as well as other Citrix products such as NetScaler ADCs, CAS, etc. The services not assessed did not meet the criteria of "in-scope" PCI DSS systems as defined by the PCI DSS Guidance for Scoping and Network Segmentation methodology.



Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Not Applicable – ADM does not store, process, and/or transmit cardholder data
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	ADM provides web-based micro services via an agent that is onboarded on Amazon Web Services' hosted environment or on customer premises that simplify application delivery infrastructure (such as NetScaler Application Delivery Controller appliances and integrates orchestration with Kubernetes), monitors performance, allows for troubleshooting, and configuration automation. The ADM agent facilitates communication between CSG customers and their deployed applications.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
Not Applicable - ADM's assessed environment is hosted with AWS	Not Applicable	Not Applicable

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Not Applicable	Not Applicable	Not Applicable	<input type="checkbox"/> Yes <input type="checkbox"/> No	Not Applicable
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	



Part 2e. Description of 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 POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

Cloud Software Group's NetScaler Application Delivery Management (ADM) is an intuitive, comprehensive platform that enables automation, orchestration, management, and analytics for application delivery across hybrid multi-cloud environments. ADM provides web-based micro services via an agent that is onboarded on Amazon Web Services' hosted environment or on customer premises that simplify application delivery infrastructure (such as NetScaler Application Delivery Controller appliances and integrates orchestration with Kubernetes), monitors performance, allows for troubleshooting, and configuration automation. The ADM agent facilitates communication between CSG customers and their deployed applications. The assessment covered AWS hosted EKS microservices, Kubernetes control plane and data plane nodes, and AWS networking, storage, compute instances (EC2), and workstations with connectivity to the in scope system components.

Does your business use network segmentation to affect the scope of your PCI DSS environment?

(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)

☒ Yes ☐ No



Part 2f. Third-Party Service Providers

Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?

☐ Yes ☒ No

If Yes:

Name of QIR Company:

Not Applicable

QIR Individual Name:

Not Applicable

Description of services provided by QIR:

Not Applicable

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?

☐ Yes ☒ No

If Yes:

Name of service provider:

Description of services provided:

Not Applicable

Not Applicable

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



Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as “Not Tested” or “Not Applicable” in the ROC.
- **None** – All sub-requirements of that requirement were marked as “Not Tested” and/or “Not Applicable” in the ROC.

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as either “Not Tested” and/or “Not Applicable” in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

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:		NetScaler Application Delivery Management (ADM)			
PCI DSS Requirement	Details of Requirements Assessed				Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None		
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<p>1.1.3 - N/A - ADM does not store, process, or transmit cardholder data, so there are no connections to cardholder data represented in the current network diagram or configurations in ADM's production environment. Consequently, dataflow diagrams for CHD or SAD is not applicable</p> <p>1.2.2 - N/A - per the AWS responsibility matrix and via review of ADM network diagrams and configurations, this is the responsibility of the cloud service provider.</p> <p>1.3.6 - N/A - ADM does not store CHD or SAD</p>
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<p>2.1.1 - N/A - there are no wireless environments connected to ADM's environment or transmitting CHD</p> <p>2.2.3 - N/A - there are no insecure services, protocols, or daemons in use</p> <p>2.6 - N/A - ADM is not a shared hosting provider</p>
Requirement 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		N/A - ADM does not store CHD or SAD
Requirement 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		N/A - ADM does not transmit CHD or SAD
Requirement 5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		5.1.2 - N/A - all ADM systems have AV installed on them, and any new systems will be evaluated if AV is necessary



Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6.4.3 - N/A - ADM does not use live production PAN within testing environments and are not present in their production environment
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.1.5 - N/A - no access is provisioned with third party personnel and all actions are monitored for remote access 8.5.1 - N/A - ADM does not have remote access into customer premises 8.7 - N/A - ADM does not store or have access to CHD within their environment
Requirement 9:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A - Physical security controls are covered by AWS and controls related to POI devices do not apply since they are not in use
Requirement 10:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10.2.1 - ADM does not have any access to CHD
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	11.1.x - N/A - there are no wireless infrastructure that can connect to or impact the security of the assessed environment, additionally AWS conducts rogue wireless access point detection for AWS infrastructure. 11.3.2 - N/A - As a PCI service provider that does not store, process or transmit CHD and as a 'security impacting' environment to their customers, the responsibility of internal penetration testing is delegated to the customer's PCI assessment.
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A - ADM is not a shared hosting provider
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A - ADM does not use POI devices with SSL or early TLS



Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	<i>November 17, 2023</i>	
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No



Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated **November 17, 2023**.

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (**check one**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>CSG-ADM</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby <i>CSG-ADM</i> has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>Compliant but with Legal exception: One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, 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 my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.


Part 3a. Acknowledgement of Status (continued)

<input checked="" type="checkbox"/>	No evidence of full track data ¹ , CAV2, CVC2, CVN2, CVV2, or CID data ² , or PIN data ³ storage after transaction authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Qualys</i>

Part 3b. Service Provider Attestation

DocuSigned by:

4B3AF3A90AFF4CC...

Signature of Service Provider Executive Officer ↑

Date: 11/27/2023

Service Provider Executive Officer Name: **Meghan Hester**Title: **Senior Director of IT Governance and Business Operations**
Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:

Jeremy Brandt (QSA) performed scope validation, interviews and observations, evidence gathering, and report generation

DocuSigned by:

D150591D733C4C5...

Signature of Duty Authorized Officer of QSA Company ↑

Date: 11/27/2023

Duty Authorized Officer Name: **Jeremy Brandt**QSA Company: **risk3sixty, LLC.**
Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:

Not Applicable

¹ Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

² The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

³ Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.



Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

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 a firewall configuration to protect cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" 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 checked="" type="checkbox"/>	<input type="checkbox"/>	

