Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022

Crowe LLP
Independent Member Crowe Global

INDEPENDENT ASSESSOR'S REPORT

To the Management of VMware LLC

We have examined VMware's compliance with PCI Data Security Standard (PCI-DSS) v3.2.1 requirements for the VMware Cloud Disaster Recovery (VCDR) platform as of March 6, 2024. Management of VMware is responsible for VMware's compliance with the specified requirements. Our responsibility is to express an opinion on VMware's compliance with the specified requirements based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether VMware complied, in all material respects, with the specified requirements referenced above. An examination involves performing procedures to obtain evidence about whether VMware complied with the specified requirements. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material noncompliance, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination does not provide a legal determination on VMware compliance with specified requirements.

In our opinion, VMware complied, in all material respects, with PCI Data Security Standard (PCI-DSS) v3.2.1 requirements as of March 6, 2024.

This report is intended solely for the information and use of the management of VMware and customers of the VCDR platform and is not intended to be and should not be used by anyone other than the specified parties.

Crowe LLP

Crowe LLP

Columbus, Ohio
March 15, 2024

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:	VMware LLC		DBA (doing business as):	VMware	
Contact Name:	Compliance		Title:	N/A	
Telephone:	(877) 486-9273		E-mail:	cloudservicescompliance@broadcom.com	
Business Address:	3401 Hillview Ave		City:	Palo Alto	
State/Province:	CA	Country:	USA	Zip:	94304
URL:	https://www.vmware.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Crowe, LLP				
Lead QSA Contact Name:	Andrew Gamble		Title:	IT Assurance Technical Senior Manager	
Telephone:	(818) 271-7584		E-mail:	andrew.gamble@crowe.com	
Business Address:	330 East Jefferson Boulevard		City:	South Bend	
State/Province:	IN	Country:	USA	Zip:	46601
URL:	https://www.crowe.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:	VMware Cloud Disaster Recovery (VCDR)	
Type of service(s) 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): Virtualized Infrastructure as a Service	**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):		

***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:	See below	
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): See below	**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:	VMware provides a number of cloud services and products that support customer CDE's, which are covered and reported on in other PCI assessments.	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Not Applicable - VMware does not have any people, processes, or technology that directly store, process, or transmit cardholder data or sensitive authentication data as part of the VCDR product architecture. As a result, VMware does not have a defined CDE. Associated requirements are considered the customer's responsibility with respect to their own CDE.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	VMware Cloud Disaster Recovery (VCDR) is part of Cloud Infrastructure Business Group (CIBG) within VMware that provides clients a comprehensive portfolio of multi-cloud infrastructure solutions, including the VCDR service. VCDR has the following components: • Scale-Out Cloud File System (SCFS) is a cloud component that enables the efficient storage of backups of the protected virtual machines in cloud storage and allows virtual machines to be recovered very quickly. • Software as a Service (SaaS) Orchestrator (Orchestrator) is a cloud component that presents a user interface to consume VCDR and includes several disaster recovery orchestration capabilities to automate the disaster recovery process.

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):
Example: Retail outlets	*3*	*Boston, MA, USA*
Not Applicable - No physical locations are in scope for this assessment. All physical security related requirements are the responsibility of Amazon Web Services (AWS). AWS is considered a key PCI service provider to VMware and is monitored for compliance per requirement 12.8.	N/A	N/A

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			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ 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.*	VMware provides cloud and virtualized datacenter services to customers. The scope of environment reviewed in this assessment are virtualized components of VCDR that are under the direct control and administration of VMware. This includes AWS Console access, virtualized network components and container based servers that facilitate the underlying infrastructure to enable customers to perform their workloads.The VCDR platform does not contain cardholder data and there is no CDE. Any other VMware product / service is not within the scope of this report
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:	
Description of services provided by QIR:	
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:**
Amazon Web Services (AWS)	Cloud Service Provider

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:	

PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	**Not Applicable:** **1.1.3, 1.2, 1.3 - VMware does not have any people, processes or technology that directly store, process, or transmit cardholder data or sensitive authentication data as part of the VCDR product architecture. As a result, VMware does not have a CDE. These requirements are considered the customer's responsibility with respect to their own CDE**
Requirement 2:	☐	☒	☐	**N/A: 2.1.1 - No wireless enviroments are in scope for the assessment** **N/A: 2.6 - Entity is not a shared hosting provider**
Requirement 3:	☐	☒	☐	**Not Applicable:** **All requirements with the exception of 3.2.1, 3.2.2, and 3.2.3, as VMware does not have any people, processes or technology that directly store, process, or transmit cardholder data or sensitive authentication data as part of the VCDR product architecture. As a result, VMware does not have a CDE. VMware does not have direct access to any customer workloads that may or may not contain CHD. These requirements are considered the responsibility of VMware's customers**
Requirement 4:	☐	☒	☐	**Not Applicable:**

				All requirements with the exception of 4.1, as VMware does not have any people, processes or technology that directly store, process, or transmit cardholder data or sensitive authentication data as part of the VCDR product architecture. As a result, VMware does not have a CDE. VMware does not have direct access to any customer workloads that may or may not contain CHD. These requirements are considered the responsibility of VMware's customer
Requirement 5:	☐	☒	☐	**Not Applicable:** **All requirements with the exception of 5.1.2 and 5.4, as all in-scope components are considered systems that are not commonly affected by malicous software**
Requirement 6:	☐	☒	☐	**Not Applicable:** **VMware does not have any people, processes or technology that directly store, process, or transmit cardholder data or sensitive authentication data as part of the VCDR product architecture. As a result, VMware does not have a CDE. VMware does not have direct access to any customer workloads that may or may not contain CHD. This requirement is considered the responsibility of VMware's customers.** **6.4.6 - No significant changes occurred relevant to this requirement for testing**
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**Not Applicable:** **8.1.5 - VMware does not grant third parties access to any of the in-scope systems/components** **8.3.1 - VMware does not have a cardholder data environment (CDE)** **8.5.1 - VMware does not have remote access to customer premises** **8.7 - VMware does not have any people, processes or technology that directly store, process, or transmit cardholder data or sensitive authentication data as part of the VCDR product architecture. As a result, VMware does not have a CDE. VMware does not have direct access to any customer workloads that may or may not contain CHD. This requirement is considered the responsibility of VMware's customers.**
Requirement 9:	☐	☐	☒	**Not Applicable:** **All in-scope components physically reside at Amazon Web Services (AWS), and corresponding physical requirements are their responsibility**
Requirement 10:	☐	☒	☐	**Not Applicable:** **10.2.1 - VMware does not have any people, processes or technology that directly store, process, or transmit cardholder data or sensitive authentication data as**

				part of the VCDR product architecture. As a result, VMware does not have a CDE. VMware does not have direct access to any customer workloads that may or may not contain CHD. This requirement is considered the responsibility of VMware's customers
Requirement 11:	☐	☒	☐	**Not Applicable:** **11.1 - All in-scope components physically reside at Amazon Web Services (AWS), and corresponding physical requirements are the responsibility of AWS.** **11.2.3 - No significant changes or vulnerabilities occurred relevant to these requirements for testing.** **11.3.4 - Segmentation is not used to isolate a CDE from other networks**
Requirement 12:	☐	☒	☐	**Not Applicable:** **12.3.10 - VMware does not have any people, processes or technology that directly store, process, or transmit cardholder data or sensitive authentication data as part of the VCDR product architecture. As a result, VMware does not have a CDE. VMware does not have direct access to any customer workloads that may or may not contain CHD. This requirement is considered the responsibility of VMware's customers**
Appendix A1:	☐	☐	☒	**Not Applicable: VMware is not a shared hosting provider**
Appendix A2:	☐	☐	☒	**Not Applicable: No POS POI terminals in scope for the assessment**

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:	*March 6, 2024*	
Have compensating controls been used to meet any requirement in the ROC?	☒ Yes	☐ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *March 6, 2024.*

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):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *VMware LLC* has demonstrated full compliance with the PCI DSS.
☐	**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 *(Service Provider Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: 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. *Check with the payment brand(s) before completing Part 4.*
☐	**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. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	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)	
☒	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.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Tenable Network Security*

Part 3b. Service Provider Attestation

DocuSigned by:
Ganesh Venkitachalam
35654D49B0914C3...

Signature of Service Provider Executive Officer ↑	*Date:* **March 15, 2024**
Service Provider Executive Officer Name: **Ganesh Venkitachalam**	*Title:* **VP of Engineering & Product Management**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	*QSA performed independent testing of PCI-DSS Version 3.2.1 requirements. See also the Independent Assessor's Report.*

DocuSigned by:
Jon Sharpe
0124CEFAC8F2471...

Signature of Duly Authorized Officer of QSA Company ↑	*Date: March 15, 2024*
Duly Authorized Officer Name: Jonathan Sharpe	*QSA Company:* Crowe LLP

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:	

[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	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐