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: RMS Australia Pty Limited

Date of Report as noted in the Report on Compliance: 22 November 2026

Date Assessment Ended: 11 November 2026

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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:	RMS Australia Pty Limited
DBA (doing business as):	RMS Australia Pty Limited
Company mailing address:	116 Harrick Road, Keilor Park, Victoria 3042
Company main website:	www.rmscloud.com
Company contact name:	Andrew Buttigieg
Company contact title:	Chief Technology Officer
Contact phone number:	+61 (3) 8399 9462
Contact e-mail address:	rocs@rmscloud.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):	N/A
Qualified Security Assessor	
Company name:	PCI Consulting Australia Pty Ltd
Company mailing address:	Suite 329/98 Elizabeth St, Melbourne, Vic, 3000
Company website:	https://www.pciconsultingaustralia.com.au
Lead Assessor name:	Daniel Warfe
Assessor phone number:	+61 (0) 459 695 900
Assessor e-mail address:	daniel.warfe@pciconsultingaustralia.com.au
Assessor certificate number:	QSA, certificate number: 206-531

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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:	RMS Cloud Services (Including 9+, Vault, IBE, Channel Manager, Guest Portal and REST API)	
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.*

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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:	N/A

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:	N/A

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.	RMS Cloud application captures cardholder data via both e-commerce and card present channel. For e-commerce (RMS Cloud platform including 9+, Vault, IBE, Channel Manager, Guest Portal and REST API): RMS Cloud accepts cardholder data from merchant customers using the RMS applications. RMS utilises a PCI DSS compliant third-party service provider VGS to manage inbound and outbound card data flows. All RMS customers are configured to route card data directly to VGS and VGS stores the card data in the VGS vault. No card data flows through the RMS

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

	infrastructure as part of the card data capture process. To process a transaction, RMS sends VGS the token and VGS initiates the payment with the merchant's payment gateway. RMS provides merchant customers the ability of seeing plain text card data and this is performed by embedding a VGS iFrame in the RMS 9+ application. RMS does not directly store, process and/or transmit any card data on any RMS managed system. For e-commerce (RMS Pay): RMS Pay accepts cardholder data from customers using the RMS applications. RMS uses PCI DSS Compliant third-party service provider Adyen, and card data is sent via an iFrame directly to Adyen. Adyen then processes and tokenizes card data and returns the token to RMS which is stored in the customers RMS database. RMS does not directly store, process and/or transmit any card data on any RMS managed system. For card-present channel: Customer can pay for the hotel room booking and other products with a debit/credit card using PCI PTS approved 4G connected POI machine. The POI machine encrypts the card data and directly transmits the encrypted card data directly to Adyen for further processing on behalf of RMS. RMS neither have access to encrypted data nor do they have decryption key, and the POI solution is supplied by Adyen. In addition, there is no mechanism available for staff from Adyen to provide remote support of EFTPOS terminals with technicians either attending the relevant location to either swap out or fix faulty terminals or a replacement being shipped to the customer.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	RMS creates the RMS application code which controls the flow of card data via iFrame or API's. RMS configures the VGS routes and the application facilitates customers using the VGS show function which allows merchant customer's to view unencrypted card data.
Describe system components that could impact the security of account data.	RMS creates the RMS Cloud application code which controls the flow of card data via an iFrame or API's. RMS configures the VGS routes which enables RMS to route card data directly to VGS. The RMS 9+ application facilitates customers using the VGS show function which allows merchant customers to view unencrypted card data via an iFrame.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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.*	RMS Cloud supports e-commerce payments through integrations with merchants' payment gateways via VGS and through RMS Pay. RMS Pay uses Adyen to process both e-commerce and card-present payments. For e-commerce through the RMS Cloud platform (including RMS 9+, Vault, IBE, Channel Manager, Guest Portal and REST API), RMS uses VGS, a PCI DSS-compliant third-party service provider, to manage inbound and outbound cardholder data flows. RMS configures the VGS routes so that cardholder data is sent directly to VGS during capture without passing through RMS-managed infrastructure. VGS stores the cardholder data in its vault. To initiate a payment, RMS sends the token to VGS, which initiates the transaction with the merchant's payment gateway. The RMS 9+ application embeds a VGS iframe that lets merchant customers use the VGS Show function to view the full PAN and expiry date. For e-commerce through RMS Pay, cardholder data is sent directly to Adyen, a PCI DSS-compliant third-party service provider, via an iframe. Adyen processes and tokenises the cardholder data and returns a token to RMS. RMS stores the token in the customer's RMS-managed database. RMS-managed systems do not directly store, process or transmit cardholder data for either e-commerce flow. For card-present payments, customers use Adyen-supplied, PCI PTS-approved, 4G-connected point-of-interaction (POI) terminals. The terminals encrypt the cardholder data and transmit it directly to Adyen for processing. RMS has no access to the encrypted cardholder data or the decryption keys. Adyen staff do not have a mechanism to provide remote support for the terminals. Faulty terminals are serviced or replaced on site, or a replacement terminal is shipped to the customer. RMS develops and maintains the RMS Cloud application code that controls cardholder data flows via iframes or APIs. RMS also configures the VGS routes and maintains the RMS 9+ integration that enables merchants to view cardholder data through the VGS Show function. The RMS Cloud application is hosted in an AWS account separate from other services. Merchant web traffic passes through the Cloudflare Web Application Firewall (WAF) before reaching the RMS applications. The AWS environment includes AWS Firewall, EC2, EKS and SQL databases.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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)
Example: Data centers	*3*	*Boston, MA, USA*
AWS	3	Australia - Sydney Europe - Frankfurt USA - N. Virginia

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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
N/A	N/A	N/A	N/A	N/A

* 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.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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:
Adyen	Payment processing and tokenization
AWS	Infrastructure hosting
Azure	Authentication services
Cloudflare	WAF and remote access to CDE
CrowdStrike	Antimalware, EDR, SOC, Incident response
VGS	CDE Hosting Provider, Payment processing and tokenization and supply of security controls

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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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: RMS Cloud Services (Including 9+, Vault, IBE, Channel Manager, Guest Portal and REST API)

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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.3.3, 2.3.1, 2.3.2 - No wireless in scope. 3.3.1.3 – There are no card-present transactions or any business process where RMS comes into contact with physical cards or track data. 3.3.2 - SAD is not stored prior to authorization. 3.3.3 - RMS is not an issuer and does not support issuing services. 3.4.2 - No RMS staff has access to full PAN. 3.5.1.1 - Hashing is not used to render PAN unreadable. 3.5.1.2, 3.5.1.3 – Disk-level or partition-level encryption is not used to store PAN data. 3.6.1.3 - RMS does not have access to clear text cryptographic components. 3.7.6 - RMS does not use manual cleartext cryptographic keys. 3.7.9 - RMS does not provide customers with encryption keys. 4.2.1.2 - No wireless in scope. 4.2.2 - No PAN is sent via messaging services. 5.2.3 , 5.2.3.1, 5.3.2.1 - All in-scope endpoints run antimalware solutions. 6.4.1 - Requirement has been superseded by 6.4.2. 8.3.9 - MFA in use. 8.3.10 - Requirement has been superseded by 8.3.10.1. 8.3.10.1 - MFA required for customer access. 8.6.1, 8.6.2 - No application or system accounts capable of interactive login were identified in the assessed environment. 9.4.6 - No paper media containing cardholder data. 9.5.1-9.5.1.3 - No POI devices. 10.4.2, 10.4.2.1 - All logs are covered in CrowdStrike and CloudWatch checks. 10.7.1 - Requirement has been superseded by 10.7.2. 11.2.2 - No wireless in scope. 11.4.7 - RMS is not a multi-tenant service provider. 12.3.2 - Customized approach was not used in this assessment. A1 - RMS is not a multi-tenant service provider. A2 - No early TLS in use
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	N/A

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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.*	17 August 2026
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	11 November 2026
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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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 *(Date of Report as noted in the ROC 2026-11-22)*.

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 *RMS Australia Pty Limited* 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 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 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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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



Signature of Service Provider Executive Officer ↗	Date: 22 November 2026
Service Provider Executive Officer Name: Andrew Buttigieg	Title: Chief Technology Officer

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: N/A



Signature of Lead QSA ↗	Date: 22 November 2026
Lead QSA Name: Daniel Warfe	



Signature of Duly Authorized Officer of QSA Company ↗	Date: 22 November 2026
Duly Authorized Officer Name: Brent Loughton	QSA Company: PCI Consulting Australia Pty Ltd

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:

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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/

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.