Payment Card Industry
Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire D for Service Providers

For use with PCI DSS Version 4.0

Revision 2

Publication Date: August 2023

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the entity's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures.* Complete all sections: The entity is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which the Attestation of Compliance (AOC) will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Self-Assessment Questionnaire (SAQ).

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Self-Assessment Questionnaire.

Part 1. Contact Information	
Part 1a. Assessed Entity	
Company name:	Razorpay Tech Solutions Private Limited
DBA (doing business as):	RTSPL
Company mailing address:	JR Cyber Laskar, Hosur Rd, Adugodi, Bengaluru, Karnataka 560030
Company main website:	https://razorpay.com/capital/
Company contact name:	Hilal Lone
Company contact title:	Senior Director, Information Security and Compliance
Contact phone number:	7006717459
Contact e-mail address:	hilal.lone@razorpay.com
Part 1b. Assessor	
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):	
Qualified Security Assessor	
Company name:	
Company mailing address:	
Company website:	
Lead Assessor Name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	

Part 2. Executive Summary

Part 2a. Scope Verification

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

Name of service(s) assessed:	Capital Services	
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): Capital Services (B2B Lending Platform)		

***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 PCI DSS Assessment (select all that apply):

Name of service(s) not assessed:	None
Type of service(s) not assessed: Not Applicable	

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):		
Provide a brief explanation why any checked services were not included in the assessment:	Not Applicable	

Part 2b. Description of Role with Payment Cards	
Describe how the business stores, processes, and/or transmits account data.	Razorpay Tech Solutions Private Limited further referred as RTSPL in this document is a B2B Lending Platform using Capital LOS. RTSPL lends loans to merchants. Razorpay Capital finances business growth through instant settlements and quick business loans. Razorpay accesses the Credit Bureaus to download the credit report of customers applying for loan and store the data available in the credit report for review and loan approval process. Report is stored for Underwriting and Analytics purposes also. The entire lending ecosystem is hosted on AWS cloud EC2 instances. AWS cloud is hosted in Mumbai, India Region. Below are total of 8 micro services of Capital application: • capital-los • capital-cards • capital-collections • capital-scorecard • capital-loc • capital-lender • capital-es • financial-data-service

		None of the above services either directly or indirectly stores, processes or transmits cardholder data.
	Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	RTSPL lends loans to merchants. Razorpay Capital powers business through Corporate Cards, Line of Credit and Instant Settlements. Below are total of 8 micro services of Capital application: • capital-los • capital-cards • capital-collections • capital-scorecard • capital-loc • capital-lender • capital-es • financial-data-service None of the above services either directly or indirectly stores, processes or transmits cardholder data.
	Describe system components that could impact the security of account data.	RTSPL lends loans to merchants. Below are total of 8 micro services of Capital application: • capital-los • capital-cards • capital-collections • capital-scorecard • capital-loc • capital-lender • capital-es • financial-data-service None of the above services either directly or indirectly stores, processes or transmits cardholder data.

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 assessment focused on below mentioned environment and technologies: ● Application Infrastructure ● Database Infrastructure ● Logging and Monitoring Solution ● Remote authentication - Palo Alto VPN and ● Jump/ Bastion server management Amazon Web Services (AWS) Cloud Infrastructure ● Classical Infrastructure management - EC2 ● Containerized Infrastructure management - EKS ● AWS IAM (Identity and Access Management) Console ● AWS Network Security Groups, Route Tables, ● NACL and VPC peering rules review ● SIEM – Coralogix ● Azure AD, AIDE, Clam AV
	Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)*	☐ Yes ✓ No

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities_for example, corporate offices, data centers, call centers, and mail rooms_in scope for the PCI DSS 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*
Cloud data center – Amazon Web Services (Reviewed via the AWS AOC)	1	Mumbai, Maharashtra, India
Head Office	1	SJR Cyber Laskar, Hosur Road, Bengaluru, Karnataka, India 560030.

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions[1♦]?

☐ 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 (YYYY-MM-DD)

[1♦] 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

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 scope of the entity's PCI DSS assessment_for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, 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 service(s) provided:
Razorpay Software Private Limited	RTSPL is using Razorpay API services, reporting services and RSPL merchant dashboard.
RazorpayX Private Limited	Payment payouts via RZPX for disbursing loans.
Amazon Web Services, Inc.	Cloud hosting services
Coralogix Ltd.	Log management solution service

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

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment

(SAQ Section 2 and related appendices)

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:

PCI DSS Requirement	Requirement Responses *More than one response may be selected for a given requirement. Indicate all responses that apply.*				
	In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
Requirement 1:	✓	☐	✓	☐	☐
Requirement 2:	✓	☐	✓	☐	☐
Requirement 3:	☐	☐	✓	☐	☐
Requirement 4:	☐	☐	✓	☐	☐
Requirement 5:	✓	☐	✓	☐	☐
Requirement 6:	✓	☐	✓	☐	☐
Requirement 7:	✓	☐	✓	☐	☐
Requirement 8:	✓	☐	✓	☐	☐
Requirement 9:	✓	☐	✓	☐	☐
Requirement 10:	✓	☐	✓	☐	☐
Requirement 11:	✓	☐	✓	☐	☐
Requirement 12:	✓	☐	✓	☐	☐
Appendix A1:	☐	☐	✓	☐	☐
Appendix A2:	☐	☐	✓	☐	☐

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.2.6 - Not Applicable as there is no services, protocols and ports are in use which is considered to be insecure. 1.3.3 - Not Applicable as wireless network is not present in scoped environment. 2.2.5 - Not Applicable as razorpay doesn't utilize any insecure services across the scoped environment. 2.3.1, 2.3.2 - Not Applicable as wireless network is not present in scoped environment. 3.3.2 - Not Applicable as SAD is not getting stored post authorization. 3.3.3 – Not Applicable as razorpay does not support the issuing services. 3.4.2 – Not Applicable as this requirement is best practice. 3.5.1.1 – Not Applicable as this requirement is best practice. 3.5.1.2 – Not Applicable as there is no removable media in scoped environment. 3.5.1.3 - Not Applicable as disk encryprion is not used in the razorpay scoped environment. 3.7.9 - Not Applicable as razorpay do not share any cryptographic key with customer. 3.1.1, 3.1.2, 3.2.1, 3.3.1, 3.3.1.1, 3.3.1.2, 3.3.1.3, 3.3.2, 3.3.3, 3.4.1, 3.4.2, 3.5.1, 3.5.1.1, 3.5.1.2, 3.5.1.3, 3.6.1, 3.6.1.1, 3.6.1.2, 3.6.1.3, 3.6.1.4, 3.7.1, 3.7.2, 3.7.3, 3.7.4, 3.7.5, 3.7.6, 3.7.7, 3.7.8, 3.7.9, 4.1.1, 4.1.2, 4.2.1, 4.2.1.1, 4.2.1.2, 4.2.2 RTSPL is not storing, processing & transmitting cardholder data. 4.2.1.1 - Not Applicable as this requirement is best practice. 4.2.1.2 - Not Applicable as razorpay doesn't utilize wireless networks for transmitting cardholder data across razorpay scoped environment. 5.2.3 - Not Applicable as there are no systems present in the scoped environment which can not be commonly affected by malware. 5.3.3 - Not Applicable as there is no removable media allowed in razorpay scoped environment. 5.3.2.1, 5.2.3.1,5.4.1- Not Applicable as this requirement is best practice. 6.3.2, 6.4.2, 6.4.3, 7.2.4, 7.2.5, 7.2.5, 7.2.5.1, 8.4.2, 8.5.1, 8.6.1 8.6.2, 8.6.3 - Not Applicable as this requirement is best practice.

	8.2.3 - Not Applicable as razorpay is not accessing their customer premises. 8.2.7 - Not Applicable as there are no third parties having access to scoped environment. 8.3.10, 8.3.10.1 – Not Applicable as customer don't have access to the crad data. 9.2.3 - Not Applicable as razorpay does not take physical media backup of cardholder data. 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3 , 9.4.4 , 9.4.5, 9.4.5.1 ,9.4.6 , 9.4.7 - Not Applicable as there are no physical media storing cardholder data. 9.5.1,9.5.1.2, 9.5.1.1 ,9.5.1.2, 9.5.1.3, 9.5.1.2.1 - Not Applicable as the scoped razorpay environment does not involve transaction and/or maintenance of POI devices. 10.4.1.1, 10.4.2.1, 10.7.2 – Not Applicable as this requirement is best practice. 11.3.1.1, 11.3.1.2, 11.4.7, 11.6.1, 11.5.1.1 - Not Applicable as this requirement is best practice. 12.3.1 ,12.3.3, 12.3.4, 12.5.2.1, 12.5.3, 12.6.2, 12.6.3.1, 12.6.3.2, 12.10.4.1 , 12.10.7 - Not Applicable as these requirement are best practice. 12.3.2 - Not Applicable as customized approach is not used for any of the requirements. Entire Appendix A1 - Not Applicable as assessed razorpay is not a shared hosting service provider. Entire Appendix A2 - Not Applicable as the scoped razorpay environment does not involve transaction and/or maintenance of POI/POS terminals.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	2023-10-20
Were any requirements in the SAQ 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 SAQ D (Section 2), dated (Self-assessment completion date *YYYY-MM-DD*).

Indicate below whether a full or partial PCI DSS assessment was completed:

- ✓ **Full** – All requirements have been assessed therefore no requirements were marked as Not Tested in the SAQ.
- ☐ **Partial** – One or more requirements have not been assessed and were therefore marked as Not Tested in the SAQ. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the SAQ D 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 SAQ are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *(Razorpay Tech Solutions Private Limited)* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company Name)* has not demonstrated compliance with the PCI DSS requirements included in this SAQ. **Target Date** for Compliance: *YYYY-MM-DD* 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 PCI DSS SAQ 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 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ 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 3a. Service Provider Acknowledgement	
Signatory(s) confirms: ***(Select all that apply)***	
✓	PCI DSS Self-Assessment Questionnaire D, Version *4.0* was completed according to the instructions therein.
✓	All information within the above-referenced SAQ and in this attestation fairly represents the results of the entity's 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	
Hilal Lone Authenticated through Leegality.com (VmwScPU) Hilal Lone Date: Fri Oct 20 11:49:05 IST 2023	
Signature of Service Provider Executive Officer	*Date: 2023-10-20*
Service Provider Executive Officer Name: **Hilal Lone**	*Title:* **Senior Director, Information Security and Compliance**

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:

Signature of Lead QSA	*Date: YYYY-MM-DD*
Lead QSA Name:	

Signature of Duly Authorized Officer of QSA Company	*Date: YYYY-MM-DD*
Duly Authorized Officer Name:	*QSA Company:*

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement	
If an ISA(s) was involved or assisted with this assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has a Non-Compliant status 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 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	✓	☐