SOC 3® – System and Organization Controls for Service Organizations:

Trust Services Criteria

Report on Razorpay Software Private Limited's System of Payment Gateway Services, relevant to Trust Services Criteria of Security, Availability and Confidentiality

For the period June 01, 2022 through May 31, 2023

Management's Report of its Assertions on the Effectiveness of Its Controls over the Payment Gateway Services Based on the Trust Services Criteria for Security, Availability, and Confidentiality.

Oct 23, 2023

We, as management of, Razorpay are responsible for:

- Identifying the Payment Gateway Services and describing the boundaries of the System, which are presented in Attachment A.
- Identifying our principal service commitments and system requirements, which are presented in Attachment B
- Identifying the risks that would threaten the achievement of our principal service commitments and service requirements that are the objectives of our System, which are presented in Attachment B
- identifying, designing, implementing, operating, and monitoring effective controls over the Payment Gateway Services to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories and associated criteria that are the basis of our assertion.

Razorpay uses Amazon Web Services (AWS) which is a third-party cloud service provider for hosting the underlying infrastructure for the Payment Gateway service. The description of the boundaries of the system presented in Attachment A indicates that complementary controls at AWS that are suitably designed and operating effectively are necessary, along with controls at Razorpay to achieve the service commitments and system requirements. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Razorpay's controls. It does not disclose the actual controls at AWS.

Razorpay performs annual due diligence procedures of the subservice organizations and based on the procedures performed, nothing has been identified that prevents us from achieving its specified service commitments.

The Description also indicates complementary user entity controls that are suitably designed and operating effectively are necessary along with Razorpay's controls to achieve the service commitments and system requirements. The Description presents Razorpay's controls and the complementary user entity controls assumed in the design of Razorpay's controls.

We assert that the controls over the System were effective throughout the period June 01, 2022 to May 31, 2023, to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus – 2022*).

Hilal Lone
Authenticated through
Leegality.com (I77knLg)
Hilal Lone
Date: Mon Oct 23 16:35:13 IST
2023

Name: Hilal Lone

Title: Chief Information Security Officer

Date: October 23, 2023.

Ernst and Young Associates LLP
12th & 13th Floor
"UB City" Canberra Block
No. 24, Vittal Mallya Road
Bengaluru - 560001, India

Tel: +91 80 6727 5000
Fax: +91 80 2201 6000

ey.com

Independent Service Auditor's Report

To: Razorpay Software Private Limited

Scope:
We have examined management's assertion, contained within the accompanying "Management's Report of its Assertions on the Effectiveness of Its Controls over the Payment Gateway Services Based on the Trust Services Criteria for Security, Availability, and Confidentiality" (Assertion), that Razorpay's controls over the Payment Gateway Services were effective throughout the period June 01, 2022 to May 31, 2023, to provide reasonable assurance that Razorpay's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in) TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*.

Razorpay uses Amazon Web Services (AWS) which is a third-party cloud service provider for hosting the underlying infrastructure for the Payment Gateway service. The description of the boundaries of the system presented at Appendix A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with related controls at Razorpay, to provide reasonable assurance that Razorpay's service commitments and system requirements are achieved based on the applicable trust service criteria. The description of the boundaries of the system presents the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS. Our procedures did not extend to the services provided by AWS, and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period June 01, 2022 to May 31, 2023.

The Description indicates that Razorpay's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Razorpay's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Management's responsibilities

Razorpay's management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Razorpay's service commitments and system requirements were achieved. Razorpay management is also responsible for providing the accompanying assertion about the effectiveness of controls within the system, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the System.
- Identifying, designing, implementing, operating and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements

Our responsibilities
Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified

Ernst and Young Associates LLP
12th & 13th Floor
"UB City" Canberra Block
No. 24, Vittal Mallya Road
Bengaluru - 560001, India

Tel: +91 80 6727 5000
Fax: +91 80 2201 6000

ey.com

Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Razorpay's relevant **security, availability, and confidentiality** policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Razorpay's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We are required to be independent of Razorpay and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Inherent limitations:

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Razorpay's service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the System or controls, or the failure to make needed changes to the System or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion:

In our opinion, Razorpay's controls over the System were effective throughout the period June 01, 2022 to May 31, 2023, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria if the complementary subservice organization and user entity controls assumed in the design of Razorpay's controls operated effectively throughout the period June 01, 2022 to May 31, 2023.

Anuj Gupta

Partner

October 23, 2023

Attachment A - Description of Boundaries of the Razorpay Software Private Limited's Payment Gateway Services

Background

Razorpay Software Private Limited (Razorpay) is a payments solution company in India that allows businesses to accept, process, and disburse payments. Razorpay provides merchants and customers access to multiple payment modes including credit / debit cards, net banking, UPI, and digital wallets. Razorpay's Payment Gateway solution integrates the merchant's existing digital processes and checkout system with a payment acquiring network via API calls to facilitate payments from Credit/Debit cards, EMIs, Net banking, UPI, and Digital wallets from affiliated banks via API integration.

Overview of Network

Razorpay's infrastructure consists of workstations, firewall, and internet connectivity used to connect to the Razorpay network. All employees and contractors are authenticated and granted access to the Razorpay environment using an active directory. Razorpay has enabled secure VPN connections for employees and contractors to connect to the Razorpay network remotely. The VPN connection is configured to encrypt network connectivity to all Razorpay applications.

Razorpay manages the operating system for servers, network, and security devices and manages software's such as anti–virus, network scanners, and log management applications.

All core applications are hosted within the datacenter located in Amazon Web Services (AWS). Razorpay provide its services to user entities using the production infrastructure hosted on Amazon Web Services (AWS), a third-party cloud service provider.

Virtual Private Cloud (VPC) is configured to segregate production and non–production instances. Perimeter firewalls are configured with firewall rules to restrict use of insecure ports / protocols. Public and private subnets are configured within the VPC to further segregate public facing hosts from other production hosts across multiple availability zones. Security groups are defined at the VPC level and applied on production instances to restrict connectivity to IP addresses which are part of the Razorpay domain. Explicit 'deny all' rule is configured within the firewall to deny all other connections.

Security protection measures are enforced to protect from Distributed Denial of Service (DDoS) and IP spoofing through the firewall. Unsafe ports / protocols are blocked through a firewall which is installed and entry / exit points to the traffic.

Public and private subnets are configured within the VPC to further segregate public facing hosts from other production hosts across multiple availability zones. Security groups are defined at the VPC level and applied on production instances to restrict connectivity to IP addresses which are part of the Razorpay domain.

To identify controls covered by the AWS service provider, we obtained an unqualified SOC 2 (Service Organization Controls Type II report and noted that the report covered sufficient controls for environmental safeguards, covered a sufficient audit period, and no exceptions were reported by an independent auditor.

Subservice Organization

Razorpay uses Amazon Web Services (AWS) which is a third-party cloud service provider for hosting the underlying infrastructure for the Payment Gateway service.

Complementary Subservice Organization Controls

Sl. No	CSOC Description	Criteria Reference
CSOC-1	Subservice organizations are responsible for obtaining attestation/assurance reports and/or certifications on a periodic basis and making them available to Razorpay.	CC1.1 CC2.3 CC3.1 CC3.2 CC4.1 CC9.2
CSOC-2	Subservice organizations are responsible for maintaining adequate physical controls to their data centre locations, as follows: ○ Implementing access control mechanisms; ○ Implementing surveillance cameras; ○ Deploying security guards.	CC6.4 CC6.7
CSOC-3	Subservice organizations are responsible for reporting incidents identified in their environments that might impact Razorpay's operations.	CC2.2 CC5.1 CC5.2 CC5.3 CC7.2 CC7.3 CC7.4 CC7.5
CSOC-4	Subservice organizations are responsible for managing backups through snapshots, patching, failure detection and recovery of the customer databases on RDS.	A1.2 A1.3
CSOC-5	Subservice organizations are responsible for availability of different zones where the customer applications and infrastructure are hosted.	A1.2 A1.3
CSOC-6	Subservice organizations are responsible for maintaining adequate environmental safeguards at their data center locations by implementing fire detection and suppression systems and carrying out preventive maintenance of the equipment on a periodic basis.	A1.2

Complementary User Entity Controls

Sl. No	CSOC Description	Criteria Reference
CUEC-1	User entities are responsible for restricting access to their merchant dashboard to authorized personnel.	CC6.1 CC6.2 CC6.3
CUEC-2	User entities are responsible for performing periodic user access review of users with access to their merchant dashboards.	CC6.1 CC6.2 CC6.3
CUEC-3	User entities are responsible for reporting security incidents of breach or loss or unauthorize disclosure of confidential data relating to the Razorpay Payment Gateway Services.	CC2.2 CC5.1 CC5.2 CC5.3 CC7.2 CC7.3 CC7.4 CC7.5
CUEC-4	User entities are responsible for performing the necessary integration, functional and compatibility related testing for the SDKs and plugins published by Razorpay to open repositories prior to integrating the same with their systems.	CC8.1

Attachment B - Principal Service Commitments and System Requirements

Razorpay has designed its overall processes and procedures to meet the objectives for its Payment Gateway services. Below is a summary of the relevant service commitments and system requirements made by Razorpay to its user entities:

- Razorpay's objectives are based on the applicable laws, regulations, compliance requirements, and service commitments made to clients that Razorpay has established for its services.
- Services include providing a technology platform to Merchants for managing transactions and settlements on their Razorpay account. The platform has modules such as transactions, settlements, invoices, payment links, payment pages, payment buttons and reports.
- Razorpay defines its terms of services, security obligations and confidentiality commitments within Service Provider Agreement and Terms & Conditions documents. The Service Provider Agreement and Terms & Conditions are accepted by merchants prior to provisioning of services.
- Razorpay establishes security, availability, and confidentiality procedures to achieve service commitments.
- As it relates to security, availability, confidentiality, Razorpay has defined Information Security Management System (ISMS) which includes policies and process around hiring, training, system design and development, implementation of appropriate administrative, technical, and physical safeguards and controls.
- The ISMS is defined to protect confidential data by implementing mechanisms for encryption and segregation of data. These requirements are communicated to Employees and Merchants via Razorpay's policies and procedures, security awareness trainings, system design documentation, and contracts with Merchants. Razorpay requires its employees, contractors, vendor partners to comply with the agreements, policies, procedures, and awareness programs of Razorpay.
- System requirements in place to meet the security, confidentiality, and availability commitments of Razorpay include, but are not limited to, the following:

    - Security principles within the fundamental designs of the applications permit users role-based access to the information required.
    - Automated tools continuously monitor and log activity, with respect to infrastructure monitoring and application performance.
    - Security groups within the cloud, to protect Razorpay systems and networks.
    - Utilizing encryption techniques when storing the data and enabling secured transmission.
    - Maintain a business continuity and disaster plan in place designed to counteract interruptions to business activities and protect critical business processes from the effects of major failures of information systems or disasters.

People

Razorpay has defined its organizational structure, reporting lines, authorities, and responsibilities as a part of its business planning process, service delivery and risk management process to meet its organizational goals and objectives along with the commitments and requirements for security, availability and confidentiality. Razorpay operates under the direction of a Chief Executive Officer (CEO) and Managing Director (MD) who are responsible for decision making and for monitoring the adherence to security, availability and confidentiality commitments at Razorpay. Razorpay has segregated personnel into various business units according to their job responsibilities. These teams are responsible for the security, availability and confidentiality of client data on network, infrastructure, applications at Razorpay.

Policies and Procedures

Razorpay has developed formal policies and procedures concerning various operational matters, including, physical and logical access controls, data classification, incident and change management, employee hiring, learning and development, performance appraisals, and terminations. Employees and contractors are made aware of these policies in accordance with Razorpay's goals and objectives to sustain its control environment.

Data

User entities' data is held in accordance with the relevant security, availability and confidentiality policies and relevant regulations, and with any specific requirements being set out in the contracts between Razorpay and user entities. Merchant and Customer data is categorized as confidential and is stored in an encrypted manner and is identifiable between individual Merchants and Customers through unique IDs.

Availability

Razorpay has established Business Continuity Management procedures for business recovery during significant disruptions. Razorpay has established formal business continuity and disaster recovery plans with guidelines, RTOs & RPOs to be achieved, number of critical resources, recovery priorities and sequences for performing recovery in case of disruptions.

The applications and databases of the Razorpay admin console within Amazon Web Services (AWS) are hosted across multiple availability zones. Auto-scaling options are configured within Amazon Web Services (AWS) to enforce high availability across the availability zones.

On an annual basis, the DevOps team performs recovery tests of its critical servers and databases and results of the tests are documented against the recovery test plan.

The DevOps and DB teams are responsible for scheduling and monitoring backup of Razorpay servers. Automated daily backups are configured within Amazon Web Services (AWS) for VMs (inclusive of application and database servers).

The uptime of the infrastructure components, utilization and performance of servers, databases, tools, and services is monitored by the respective Business Units (BU's).

Razorpay undergoes an external assessment to assess compliance against RBI and NPCI data localization requirements.

Confidentiality

Razorpay defines its terms of services, security obligations and confidentiality commitments within its Service Agreement and Terms and Conditions. The Merchant Agreement, and Terms and Conditions are available on Razorpay's website and are digitally accepted by Merchants prior to provisioning of services.

Razorpay has established a segregated environments for the production and stage. Further, Card Data and Non-Card Data is segregated between independent clusters on Amazon Web Services (AWS).

Internally, confidentiality requirements are communicated to employees through training and policies. At the time of onboarding, new joiners are required to read and sign an acknowledgement that they have read, understood, and agreed to comply with Razorpay's Non-Disclosure Agreements (NDA).

Razorpay has defined a Clear Desk and Clear Screen Policy which is applicable to hardcopies, laptops, desktops, removable storage media devices and information processing systems.

Razorpay has enabled encryption on end point devices. Razorpay has enabled encryption for data stored on the RDS instances.