Postman, Inc.
Type 2 SOC 3
2021

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

September 1, 2020 to February 28, 2021

Table of Contents

SECTION 1 ASSERTION OF POSTMAN, INC. MANAGEMENT 1

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT 3

SECTION 3 POSTMAN, INC.'S DESCRIPTION OF ITS POSTMAN API DEVELOPMENT PLATFORM SYSTEM THROUGHOUT THE PERIOD SEPTEMBER 1, 2020 TO FEBRUARY 28, 2021 7

OVERVIEW OF OPERATIONS 8
Company Background 8
Description of Services Provided 8
Principal Service Commitments and System Requirements 8
Components of the System 8
Boundaries of the System 10
Changes to the System in the Last 12 Months 10
Incidents in the Last 12 Months 10
Criteria Not Applicable to the System 10
Subservice Organizations 10
COMPLEMENTARY USER ENTITY CONTROLS 12

SECTION 1

ASSERTION OF POSTMAN, INC. MANAGEMENT

ASSERTION OF POSTMAN, INC. MANAGEMENT

April 30, 2021

We are responsible for designing, implementing, operating, and maintaining effective controls within Postman, Inc.'s ('Postman' or 'the Company') Postman Application Program Interface ('API') Development Platform System throughout the period September 1, 2020 to February 28, 2021, to provide reasonable assurance that Postman's service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented below in "Postman, Inc.'s Description of Its Postman API Development Platform System throughout the period September 1, 2020 to February 28, 2021" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 1, 2020 to February 28, 2021, to provide reasonable assurance that Postman'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* (AICPA, *Trust Services Criteria*). Postman's objectives for the system in applying applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Postman, Inc.'s Description of Its Postman API Development Platform System throughout the period September 1, 2020 to February 28, 2021".

Postman uses Amazon Web Services ('AWS') to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Postman, to achieve Postman's service commitments and system requirements based on the applicable trust services criteria. The description presents Postman's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Postman's controls. The description does not disclose the actual controls at the subservice organization.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period September 1, 2020 to February 28, 2021 to provide reasonable assurance that Postman's service commitments and system requirements were achieved based on the applicable trust services criteria.

Shamasis Bhattacharya
Vice President of Engineering
Postman, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Postman, Inc.:

Scope

We have examined Postman, Inc.'s ('Postman' or 'the Company') accompanying description of Postman API Development Platform System titled "Postman, Inc.'s Description of Its Postman API Development Platform System throughout the period September 1, 2020 to February 28, 2021" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period September 1, 2020 to February 28, 2021, to provide reasonable assurance that Postman'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* (AICPA, *Trust Services Criteria*).

Postman uses AWS to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Postman, to achieve Postman's service commitments and system requirements based on the applicable trust services criteria. The description presents Postman's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Postman's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Postman is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Postman's service commitments and system requirements were achieved. Postman has provided the accompanying assertion titled "Assertion of Postman, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Postman is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description 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 our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Postman's Postman API Development Platform System were suitably designed and operating effectively throughout the period September 1, 2020 to February 28, 2021, to provide reasonable assurance that Postman's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on Postman's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Postman, user entities of Postman's Postman API Development Platform during some or all of the period September 1, 2020 to February 28, 2021, business partners of Postman subject to risks arising from interactions with the Postman API Development Platform, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
April 30, 2021

SECTION 3

POSTMAN, INC.'S DESCRIPTION OF ITS POSTMAN API DEVELOPMENT PLATFORM SYSTEM THROUGHOUT THE PERIOD SEPTEMBER 1, 2020 TO FEBRUARY 28, 2021

OVERVIEW OF OPERATIONS

Company Background

Postman was founded in 2014 with the goal of making it easier to work with application programming interfaces (APIs). Today, Postman is a global company with major offices in San Francisco (where the company is headquartered) and Bangalore, with additional employees throughout the world.

The system in-scope for this report is primarily software as a service (SaaS). The system comprises the Postman API Platform (hosted by Amazon Web Services) along with the platform's supporting IT infrastructure and business processes.

Description of Services Provided

Postman is a collaboration platform for API development. Postman's features simplify each step of building an API and streamline collaboration so that software developers (and their organizations) can create better APIs - faster.

Principal Service Commitments and System Requirements

Postman provides SaaS to its users to manage entire life cycle of API design, development and management-as such it strives to adhere to provide software service availability and reliability to perform the said objectives while operating under, but not limited to, appropriate regulatory recommendations from relevant governing bodies.

Security commitments to user entities are documented and communicated in Service Level Agreements ('SLAs') and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Protection of private data stored on remote Postman systems
- Access control of data among various roles within an organization based on their preferences
- Retention of data for agreed-upon retention policies

Postman establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Postman's system policies.

Components of the System

Infrastructure

Primary infrastructure used to provide the Postman API Platform includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Servers	AWS-EC2	Hosts Postman developed web application
Load Balancers	AWS-ELB	Evenly distributes traffic across multiple servers
Databases	AWS- Relational Database Service ('RDS')	Serves as long term storage for data.
Caches	AWS-ElastiCache	Used as an ephemeral, in-memory store for data.

Software

Primary software used to provide the Postman API Platform includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Node.js	Alpine Linux 3	Runtime environment for application servers.
Electron	cross platform	JavaScript application build platform
Docker	Amazon Linux 2	Container tool used to achieve isolation.
NGINX		Reverse proxy for application servers.
MySQL	Linux	Database engine for persistent storage.
Redis		Database engine for in-memory ephemeral storage.
Pingdom	Vendor Hosted	Monitoring tool
New Relic		Monitoring tool
JIRA		Ticketing system for incidents and change management.

People

The Postman staff provides support for the above services in each of the following functional areas:

- Management: Responsible for providing general oversight and strategic planning of operations
- Engineering: Responsible for handling the development of the product along with creation and maintenance of technical operational infrastructure
- Information Technology (IT): The IT team is responsible for providing infrastructure, networking, and IT system administration which directly supports the company and services provided
- Information Security and Assurance: Responsible for ensuring secure development and delivery of product and services while maintaining compliance with applicable regulations
- Customer Success: Responsible for serving customers by providing product and service information that includes resolving product and service issues
- People Operations (Ops): Responsible for human resources management and its allied systems and policies
- Marketing: Responsible for promoting the Postman brand and business along with alignment towards positive sales of products or services
- Developer Relations: Responsible for building positive relationships with Developers using the product

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other relevant regulations, with specific requirements formally established in customer contracts. Customer data is captured, which is utilized by Postman in delivering its technology solutions. Such data includes, but is not limited to, the following:

1. Alert notifications and monitoring reports generated from monitoring applications.
2. Alert notifications received from automated backup systems.
3. Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, intrusion detection system (IDS) alerts, or automated patching systems.
4. Incident reports documented via JIRA and other corporate intranet documents.

Customer data is processed and securely stored with technical and administrative controls which include role based access founded on the principle of need to know and least privilege. Access is approved prior to provisioning and is periodically reviewed to ensure appropriateness.

Processes, Policies and Procedures

Formal policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. The teams are expected to adhere to the Postman policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Postman team member.

Boundaries of the System

The scope of this report includes the Postman API Platform performed in the San Francisco, California and Bangalore, India facilities.

This report does not include the data center hosting services provided by AWS at multiple facilities.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common/Security, Availability, and Confidentiality criterion were applicable to the Postman API Platform.

Subservice Organizations

This report does not include the data center hosting services provided by AWS at multiple facilities.

Subservice Description of Services

AWS provides data center hosting services, which includes implementing physical security controls and environmental controls to protect the housed in-scope systems. Controls include, but are not limited to, visitor sign-ins, required use of badges for authorized personnel, and monitoring and logging of the physical access to the facilities.

Complementary Subservice Organization Controls

Postman's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Postman's services to be solely achieved by Postman control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Postman.

The following subservice organization controls should be implemented to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Security	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual. Physical access is revoked within 24 hours of the employee or vendor record being deactivated. Physical access to data centers is reviewed on a quarterly basis by appropriate personnel. Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations. Physical access points to server locations are managed by electronic access control devices.
Security, Confidentiality	CC6.5, C1.2	AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Security Zones.
		AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.
		AWS retains customer content per customer agreements.
Availability	A1.1	Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems. Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels. Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers. Amazon-owned data centers have generators to provide backup power in case of electrical failure.

Postman management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Postman performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and the subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Postman's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Postman's services to be solely achieved by Postman control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Postman's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Postman.
2. User entities are responsible for keeping key personnel and contact information up to date.
3. User entities are responsible for updating pertinent account information in a timely manner.
4. User entities are responsible for notifying the entity of any changes to the confidentiality practice.
5. User entities are responsible for notifying Postman of changes made to technical or administrative contact information.
6. User entities are responsible for ensuring notification lines for reporting failures and errors are up to date.
7. User entities are responsible for protecting user credentials.
8. User entities are responsible for segregating user access to the entities system.
9. User entities are responsible for notifying the entity of any malicious or suspicious events from the system.
10. User entities are responsible for maintaining their own system of record.
11. User entities are responsible for ensuring the supervision, management, and control of the use of Postman services by their personnel.
12. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Postman services.
13. User entities are responsible for providing Postman with a list of approvers for security and system configuration changes for data transmission.
14. User entities are responsible for immediately notifying Postman of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.