COALFIRE CONTROLS

Report on Google LLC's Description of Its Apigee Edge API Management Platform and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality Throughout the Period April 1, 2022 to March 31, 2023

SOC 2® - SOC for Service Organizations: Trust Services Criteria

Google

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Google LLC ("Google")

Scope

We have examined Google's accompanying description in Section 3 titled "Google LLC's Description of Its Apigee Edge API Management Platform Throughout the Period April 1, 2022 to March 31, 2023" (description) based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022*) (2018 description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Google'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)* (2017 TSC).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Google, to achieve Google's service commitments and system requirements based on the applicable trust services criteria. The description presents Google's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Google's controls. 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 controls.

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

Service Organization's Responsibilities

Google 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 Google's service commitments and system requirements were achieved. In Section 2, Google has provided the accompanying assertion titled "Assertion of Google LLC Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Google 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.

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

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

- 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 report users may consider important to meet their informational needs. There are inherent limitations in 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 or 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.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, “Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories” of this report.

Opinion

In our opinion, in all material respects—

a. The description presents Google’s Apigee Edge API Management Platform that was designed and implemented throughout the period April 1, 2022 to March 31, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Google’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Google’s controls throughout that period.

c. The controls stated in the description operated effectively throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Google’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Google’s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Google, user entities of Google’s Apigee Edge API Management Platform during some or all of the period April 1, 2022 to March 31, 2023, business partners of Google subject to risks arising from interactions with Google’s Apigee Edge API Management Platform, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and 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.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization’s service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties. If a report recipient is not a specified party as defined above and has obtained this report, or has access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Coalfire Controls, LLC as a result of such access. Further, Coalfire Controls, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Coalfire Controls LLC

Greenwood Village, Colorado
May 23, 2023

Section 2

Assertion of Google LLC Management

Google LLC
1600 Amphitheatre
Parkway
Mountain View, CA 94043

650 253-0000 main
Google.com

Assertion of Google LLC ("Google") Management

We have prepared the accompanying description in Section 3 titled "Google LLC's Description of Its Apigee Edge API Management Platform Throughout the Period April 1, 2022 to March 31, 2023" (description), based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* (2018 description criteria). The description is intended to provide report users with information about the Apigee Edge API Management Platform that may be useful when assessing the risks arising from interactions with Google's system, particularly information about system controls that Google has designed, implemented and operated to provide reasonable assurance that its 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)* (2017 TSC).

Google uses subservice organizations for IaaS services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Google, to achieve Google's service commitments and system requirements based on the applicable trust services criteria. The description presents Google's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Google's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Google, to achieve Google's service commitments and system requirements based on the applicable trust services criteria. The description presents Google's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Google's controls.

We confirm, to the best of our knowledge and belief, that:

a. The description presents Google's Apigee Edge API Management Platform that was designed and implemented throughout the period April 1, 2022 to March 31, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Google's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities

applied the complementary controls assumed in the design of Google's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Google's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Google's controls operated effectively throughout that period.

Google LLC

Section 3

Google LLC's Description of Its Apigee Edge API Management Platform Throughout the Period April 1, 2022 to March 31, 2023

Overview of Operations

The Google LLC (“Google” or “the Company”) Apigee Edge Application Programming Interface (API) Management Platform (“Apigee Edge”) is a Google Cloud product that is intended to enable enterprises to secure, manage, scale, and analyze their digital businesses. The core API management product includes a mediation and intelligence engine, developer services, and monitoring and reporting services. Together, these services help provide a foundation for enterprises to leverage existing systems, shared databases, security frameworks, management infrastructure, and operational tools. Apigee Edge also includes bot detection and prevention capabilities that enable blocking or throttling bad bot traffic based on the analysis of billions of API calls using machine intelligence. Monetization capabilities work to enable companies to extract value from APIs.

Apigee Edge helps businesses adapt quickly by unlocking the value of data and delivering modern applications. This gives businesses control over and visibility into the APIs that connect applications and data across the enterprise and across clouds. Apigee Edge also works to enable businesses to securely expose their digital assets through APIs for developers and partners who are building applications. This allows enterprises to measure the success of their digital initiatives with end-to-end analytics.

Figure 1: Apigee Edge Overview

Developer Ecosystems

Apigee Edge’s developer ecosystems layer works to enable a developer and community experience that accelerates API adoption, simplifies learning, and increases the business value of APIs.

A developer portal is deployed by an enterprise to provide a community for developers with the resources necessary to learn about the enterprise’s APIs, become a registered developer, and collaborate with both peers and the enterprise. Tools such as blogs, frequently asked questions (FAQs), and forums help developers interact with one another to present solutions. Modeling and developer management helps provide streamlined developer registration with a manual or automatic registration process.

Developer keys can be approved automatically or manually for a given API product. Interactive API documentation and modeling through Apigee Edge’s SmartDocs feature supports the design and documentation of new APIs, as well as learning, testing, and evaluating existing APIs. In addition, terms of service (TOS) and acceptance for APIs can be managed.

Monitoring and Reporting

Apigee Edge's monitoring and reporting layer works to enable end-to-end visibility across the digital value chain with the unified operational, developer, application performance, and business metrics necessary to help monitor, measure, and manage success.

This API analytics solution helps customers make better business decisions through an understanding of customer behavior and interactions using real-time data from their APIs and the edge of their business. Business metrics help provide organizations with a complete picture of their customers, including how those customers use their services with partner APIs, social networks, and other products.

Operational analytics monitor the health and performance of production APIs, working to enable enterprises to plan for traffic spikes, identify slow and error-prone APIs, find root causes, and understand traffic anomalies. Application performance monitoring is intended to measure mobile application usage and the performance of applications on different platforms, carriers, and devices. Customers can segment their audience by top developers and applications, understand usage by API method to know where to invest, create custom reports on business-level information, and see long-term usage trends.

Mediation and Intelligence Engine

Apigee Edge's mediation and intelligence engine layer is intended to unite both Internet and enterprise technologies with API management, security, and programming extensibility.

API management enables the transformation of existing back-end services to APIs with over 40 policies designed for "configure rather than code" deployment. A unified security model is provided throughout the platform to help provide secure portal access and support other pre-existing security programs by using pluggable authentication. Apigee Edge allows for the extension of mediation and intelligence engine capabilities by offering support for Java, JavaScript, Node.js, and Python.

The system description in this section of the report details Apigee Edge. Any other Google services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at Google and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organizations).

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of Apigee Edge. Commitments are documented and communicated in the Google TOS for Apigee Edge Products and the Data Processing and Security Terms for Apigee Edge Products. The Company's principal service commitments related to Apigee Edge include the following:

- Google will provide technical support for customers according to the technical support guidelines, which can be found at https://cloud.google.com/terms/apigee-support (as of the date of this report).
- Google will implement technical and organizational measures to safeguard customers' content from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.
- Google will implement and maintain technical and organizational measures to help ensure the ongoing availability, confidentiality, and resilience of Google's systems and services.

- Google will not disclose confidential information, except to those who have a business need to know it to fulfill the services and have agreed in writing to keep the information confidential.
- Google will notify customers promptly and without undue delay after becoming aware of a data incident and promptly take reasonable steps to minimize harm and secure customer data.

System requirements are specifications regarding how Apigee Edge should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures, which are available to all employees. The Company's system requirements related to Apigee Edge include the following:

- Employee provisioning and deprovisioning standards
- Logical access controls, such as the use of user IDs and passwords to access systems
- Protection of data in transit
- Risk assessment and risk mitigation standards
- System monitoring
- Change management procedures
- Business continuity planning and testing
- Encryption standards
- Intrusion detection standards
- Incident response procedures

The Components of the System Used to Provide the Services

The boundaries of Apigee Edge are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of Apigee Edge.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

Core system components for the service are located in Google Cloud Platform (GCP), a separate service offering of Google, and Amazon Web Services (AWS). Apigee Edge utilizes multiple regions and multiple availability zones within each region for redundancy and disaster recovery purposes to help ensure the availability of the platform.

Software

Software consists of the programs and software that support Apigee Edge (operating systems [OSs], middleware, and utilities). Apigee Edge's proprietary platform architecture is comprised of application and database servers running the Linux OS. Apigee Edge runs on Linux CentOS, on which Apigee Edge's software is installed. These are managed by Apigee Edge operations. Big Query, MySQL, Cassandra, and Zookeeper are used to manage and store configuration and analytics data. Apigee Edge's source code is

built on various technologies, including Cassandra, Qpid, Graphite, Go, Amazon Elasticsearch Service (Elasticsearch), Node.js, PostgreSQL, Kubernetes, and Spark.

People

Google develops, manages, and secures Apigee Edge via separate departments. The responsibilities of these departments are defined as follows:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
Operations Management	Responsible for day-to-day management of the platform, including ensuring and defining platform availability and security.
Software Development	Responsible for new application version releases and support for internally escalated issues from operations departments.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Apigee Edge only stores customer data that is required for user authentication and the configuration of user services. Apigee Edge's use of databases is limited to storing policies, configurations, and approved keys, in addition to any analytics metadata that the customer wants collected.

Data in use and at rest is located at GCP and AWS, which provide infrastructure as a service (IaaS) to the Company. The geographical locations of data are summarized in the following table:

Data		
Region	**AWS**	**GCP**
US – East	Virginia (us-east-1)	South Carolina (us-east1)
US – Central	N/A	Iowa (us-central1)
US – West	Oregon (us-west-2)	Oregon (us-west1)
Canada	N/A	Montreal (northamerica-northeast1)
SA – Brazil	Sao Paulo (sa-east-1)	Sao Paulo (southamerica-east1)
EU – Ireland	Ireland (eu-west-1)	N/A
EU – London	N/A	London (europe-west2)
EU – Frankfurt	Frankfurt (eu-central-1)	Frankfurt (europe-west3)
EU – Belgium	N/A	Belgium (europe-west1)
EU – Finland	N/A	Finland (europe-north1)
AP – Australia	Sydney (ap-southeast-2)	Sydney (australia-southeast1)

Data		
Region	**AWS**	**GCP**
AP – Singapore	Singapore (ap-southeast-1)	Singapore (asia-southeast1)
AP – Japan	Tokyo (ap-northeast-1)	Tokyo (asia-northeast1)
AP – India	N/A	Mumbai (asia-south1)
AP – Hong Kong	N/A	Hong Kong (asia-east2)

System Incidents

Google provides incident reporting and informs the affected parties and the public of system impacts that may affect their processing via public-facing websites. Google protects the confidentiality of information concerning individual cloud customers when reporting incidents. There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements during the period from April 1, 2022 to March 31, 2023.

The Applicable Trust Services Criteria and Related Controls

Applicable Trust Services Criteria

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- *Security*: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability or confidentiality of information or systems and affect the entity's ability to meet its objectives.
- *Availability:* Information and systems are available for operation and use to meet the entity's objectives.
- *Confidentiality*: Information designated as confidential is protected to meet the entity's objectives.

Many of the criteria used to evaluate a system are shared amongst all in-scope categories; for example, the criteria related to risk assessment apply to the security, availability, and confidentiality categories. As a result, the criteria for the security, availability, and confidentiality categories are organized into (a) the criteria that are applicable to all categories (common criteria) and (b) criteria applicable only to a single category. The common criteria constitute the complete set of criteria for the security category. For the categories of availability and confidentiality, a complete set of criteria is comprised of all the common criteria and all the criteria applicable to the category being reported on.

The common criteria are organized as follows:

1. *Control environment:* The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.

2. *Information and communication:* The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
3. *Risk assessment:* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
4. *Monitoring activities:* The criteria relevant to how the entity monitors the system, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.
5. *Control activities:* The criteria relevant to the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
6. *Logical and physical access controls:* The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. *System operations:* The criteria relevant to how the entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations.
8. *Change management:* The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
9. *Risk mitigation:* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the security, availability, and confidentiality categories. The Company has elected to exclude the processing integrity and privacy categories.

As defined by the American Institute of Certified Public Accountants (AICPA), internal control is a process effected by an entity's board of directors, management, and other personnel and consists of five interrelated components:

- Control Environment – Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- Risk Management – The entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks should be managed across the internal and external control environment, including third-party risk.
- Information and Communication – Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange information needed to conduct and control its operations.
- Monitoring – The entire process must be monitored, with modifications made, as necessary. In this way, the system can react dynamically, changing as conditions warrant.
- Control Activities – Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to the achievement of the entity's control objectives are effectively carried out.

This section briefly describes the essential characteristics and other interrelated components of internal controls and divides them into four broad areas. These areas support the achievement of the applicable Trust Services Criteria for security, availability, and confidentiality as they pertain to the Apigee Edge products that may be relevant to customers. They include the following:

- Policies (Control Environment and Risk Management) – The entity has defined and documented its policies relevant to the particular objective.
- Communications (Information and Communication) – The entity has communicated its defined policies to responsible parties and authorized users of the system.
- Procedures (Control Activities) – The entity has placed procedures into operation to achieve its objectives in accordance with its defined policies.
- Monitoring (Monitoring Activities) – The entity monitors the system and takes action to maintain compliance with its defined policies.

Policies

Internal Control Environment

Integrity and Ethical Values

Internal Control Environment

Google has designed its internal control environment with the objective of providing reasonable, but not absolute, assurance as to the security, availability, and confidentiality of the financial and user information, as well as the protection of assets from unauthorized use or disposition. Management has established and maintains an internal control structure that monitors compliance with established policies and procedures.

Google has established internal compliance teams utilizing scalable processes to efficiently manage core infrastructure and product-related security, availability, and confidentiality controls.

To maintain internal compliance, Google has established a disciplinary process for non-compliance with the Code of Conduct, security policy, and other personnel requirements that could include dismissal, lawsuits, or criminal prosecution.

With regard to the effect of the COVID-19 pandemic, there were no significant changes to Apigee Edge that resulted in the failure to meet principal service commitments and system requirements. Google has utilized existing technologies to migrate the workforce to a remote work environment, sustaining all business processes not requiring physical access to facilities. Functions requiring physical access to computer equipment and other hardware have undergone staff adjustments in order to maintain business operations and ensure the safety of personnel.

System Requirements

Google has established internal policies and processes to support the delivery of Apigee Edge to customers. These internal policies are developed in consideration of legal and regulatory obligations, and they define Google's organizational approach and system requirements. The delivery of these services depends on the appropriate functioning of system requirements defined by Google.

The following processes and system requirements function to meet Google's contractual commitments to customers with respect to the processing and security of information assets:

- Access Security: Google maintains data access and logical security policies designed to prevent unauthorized persons or systems from gaining access to systems used to host the Apigee Edge environment. Access to systems is restricted based on the principle of least privilege.
- Change Management: Google requires standard change management procedures to be applied during the design, development, deployment, and maintenance of all Google applications, systems, and services.
- Incident Management: Google monitors a variety of communication channels for security incidents, and Google's security personnel react promptly to known incidents.
- Data Management: Google complies with any obligations applicable to it with respect to the processing of personal data. Google processes data in accordance with the customer instructions and complies with applicable regulations.
- Data Security: Google implements and maintains technical and organizational measures to protect information assets against accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access.
- Third-Party Risk Management: Google conducts routine inspections of subprocessors to evaluate control conformance. Google defines security and privacy practices that must be applied to the processing of data and obtains contractual commitments from subprocessors to comply with these practices.

Hiring Practices

Google has designed formal global hiring practices to help ensure that new, rehired, or transferred employees are qualified for their functional responsibility. Where local labor law or statutory regulations permit, Google may conduct criminal, credit, or security checks on all potential employees, as well as verification of the individual's education, previous employment, and referrals. The specifics or extent of the background checks performed depend on the position and location for which the individual is applying.

Upon acceptance of employment, all employees are required to execute a confidentiality agreement, as well as acknowledge receipt and compliance with Google's Employee Handbook. The confidentiality and privacy of customer data is emphasized in the handbook and also during new employee orientation. It is the responsibility of every Google employee to timely communicate significant issues and exceptions to an appropriate higher level of authority within the Company. Every employee has a written job description, and every job description lists qualifications, such as requisite skills and experience, that candidates must meet in order to be hired by Google.

Risk Management

Risk management is a pervasive component of the Apigee Edge products provided by Google to user entities, irrespective of the location or business area. The Google teams that lead engineering, sales, customer service, finance, and operations have the primary responsibility to understand and manage the risks associated with their activities for user entities using Apigee Edge. These risk management and mitigation activities are so critical that they have also been integrated into Google's repeatable process model, which is utilized daily.

At a corporate level, there are multiple functional areas that provide risk management support through policy guidelines and internal consulting services. These areas include legal, information security, internal audit, privacy engineering, and engineering compliance.

Google develops and maintains a risk management framework to manage risk to an acceptable level for Apigee Edge. Google has developed vulnerability management guidelines and regularly analyzes the vulnerabilities associated with the system environment. Google takes into consideration various threat sources such as insider attacks, external attacks, errors, omissions, and third party-related issues such as the inadvertent disclosure of Google's confidential information (e.g., payroll data) by a third party.

Factors, including the threat-source motivation and capability, nature of the vulnerability, and existence and effectiveness of current controls, are considered in determining the probability that a potential vulnerability may be exercised. Google designates the likelihood that a potential vulnerability could be exercised by a given threat-source as high, medium, or low.

Google then determines the potential adverse impact resulting from the successful exploitation of vulnerabilities. The highest priority is given to any potential compromise of user data.

The level of risk and remediation priority for a particular threat or vulnerability pair is expressed as a function of the following:

- The likelihood of a given threat-source's attempt to exploit a given vulnerability
- The impact should a threat-source successfully exercise the vulnerability
- The effectiveness of existing security controls for reducing or eliminating risk

Google performs a formal risk assessment at least annually and determines the likelihood and impact of identified risks using qualitative and quantitative methods. The likelihood and impact associated with each risk is determined independently by considering each risk category. Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented, and approved by management.

Google has an established Internal Audit function and compliance specialists responsible for evaluating the effectiveness of controls in addressing a given risk, including, among other controls, identity management, source code management, and authentication infrastructure controls against requirements. They perform risk-based assessments and issue audit reports regarding their analysis. The remediation of security deficiencies is tracked through internal tools.

Third-Party Risk Management

Google has a dedicated Third-Party Security and Privacy Management team to manage third-party risks. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure that they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms. Google defines security and privacy practices that must be applied to the processing of data and obtains contractual commitments from subprocessors to comply with these practices.

Google may utilize third-party vendors to support Apigee Edge. New vendors are subject to Google's Vendor Security Assessment (VSA) process, a risk-based program led by the Security team to review the security practices of vendors and the security posture of vendor products prior to onboarding.

A subset of vendors is considered to be subprocessors based on the data sharing relationship between the vendor and Google. Google utilizes subprocessors to support Apigee Edge and has established expectations for subprocessors related primarily to security. The meeting of these expectations is subject to periodic review by Google.

Google evaluates conformance to these expectations through the inspection of third-party SOC 2 reports, inclusive audit testing, and communications in a governing body consisting of compliance personnel from Google and relevant third parties. If Google identifies any deviations in the performance of subprocessor controls, findings are evaluated by Google and discussed with the vendor upon completion of the audit. When applicable, remediation plans are put in place to timely resolve issues.

Google has also implemented a Subprocessor Data Processing Agreement (SDPA) in contracts with subprocessors. The SDPA defines the security and privacy obligations that the subprocessor must meet to satisfy Google's obligations regarding customer data prior to Google granting such access.

Data Confidentiality

Google has established training programs for privacy and information security to support data confidentiality. All employees are required to complete these training programs annually. All product feature launches that include a new collection, processing, or sharing of user data are required to go through an internal design review process. Google has also established incident response processes to report and handle events related to confidentiality.

Other Considerations

Formal organizational structures exist and are available to Google employees on the Company’s intranet. The intranet provides drill-down functionality for identifying employees in the Functional Operations team. Google has developed and documented formal policies, procedures, and job descriptions for operational areas, including data center operations, security administration, system and hardware change management, hiring, training, performance appraisals, terminations, and incident escalation. These policies and procedures have been designed to segregate duties and enforce responsibilities based on job functionality. Google has also developed the Data Security Policy, Data Classification Guidelines, and Security Labels for Google Information to establish procedures for information labeling and handling in accordance with the Google guidelines.

Policies and procedures are reviewed and updated, as necessary. Databases and websites track and monitor the progress of Apigee Edge project developments. Google establishes agreements, including non-disclosure agreements, for preserving the confidentiality of information and software exchange with external parties.

Communications

Information and Communication

To help align its business strategies and goals with operating performance and controls, Google has implemented various methods of communication to ensure that all interested parties and personnel understand their roles and responsibilities and to ensure that significant events are communicated in a timely manner. These methods include:

- Orientation and training programs for newly hired employees
- An information security training program to be completed upon hire.

- A code of conduct training program to be completed upon hire. Management monitors employees' compliance with an online learning system.
- Regular management meetings for updates on business performance and other business matters
- Company goals and responsibilities to be developed and communicated by management at least annually. Results of previous goals are evaluated and communicated to employees.
- Detailed job descriptions; product information (including the system and its boundaries); and Google's security, confidentiality, and availability obligations that are made available to employees on the intranet
- The use of email to communicate time-sensitive messages and information
- Publishing security policies and security-related updates on its intranet, which is accessible by all Google employees, temporary workers, contractors, and vendors

Google has also implemented various methods of communication to help ensure that user entities understand Google's commitments to security, availability, and confidentiality for Apigee Edge. These methods help ensure that significant events are communicated to user entities in a timely manner.

A description of Apigee Edge is documented and made available to authorized internal and external users through ongoing communications with customers or official blog postings. The primary conduit for communication is the Google website, which is made available to all user entities. This includes blog postings on the official Google blog and various Apigee Edge–specific blogs, support forums, and release notes. Google provides 24/7 assistance, including online and phone support, to address customers' concerns. Customer service and technical support representatives are also an important communication channel, as they maintain records of problems reported by the user entity. Customer service representatives also assist in communicating information regarding new issues or developments, changes in services, and other information. Google maintains an established board of directors that operates independently from management. The board exercises oversight over management decisions.

Procedures

Information Security Program

Google's Information Security program is designed to safeguard information assets against unauthorized use, disclosure, modification, damage, or loss. The program includes educating Google personnel about security related issues, assessing current policies and developing new policies, assisting in strengthening technical measures to protect corporate resources, and developing mechanisms to react to incidents and events that could affect Google's information assets.

Google has dedicated security teams responsible for educating Google personnel about security and assisting product teams with security design. Information security is managed by a dedicated security executive who is independent of information technology (IT) management responsibilities and may escalate security issues or concerns directly to the board. The Security team also reviews the security practices of vendors and the security posture of vendor products for all vendors with whom Google shares confidential or sensitive information.

Google's security policies have been reviewed and approved by management and are published and communicated to employees and vendors with access to the Google environment. Google's security policies describe security objectives, provide a security framework, and emphasize the importance of security to Google's business. Security policies are reviewed at least annually. Policies, FAQs, and guidelines are updated, as needed.

Mobile Device Management

Google has established policies to manage mobile device security. These policies list the approved devices, applications, and software, as well as cover device encryption, compatibility, jailbreaking, and mobile security. The acceptable usage and requirements for all mobile devices are documented and are communicated through Google's security awareness and training program.

Authentication, Authorization, and Administration

Strong authentication and access controls are implemented to restrict access to production systems, internal support tools, and customer data. Machine-level access restriction relies on a Google-developed distributed authentication service based on Transport Layer Security (TLS) certificates that help to positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. Google uses encryption to secure user data in transit between Google production facilities. Access to internal support tools, those used by Google operational staff to maintain and troubleshoot the systems for Apigee Edge is controlled via Access Control Lists (ACLs), thus limiting the use of these tools to only those individuals that have been specifically authorized.

Digital certificates used for machine authentication and data encryption are issued by an internal Google certificate authority. Encryption is used to protect user authentication and administrator sessions transmitted over the internet. Remote access to the Google corporate machines requires a Google issued digital certificate installed on the connecting device and two-factor authentication.

Both user and internal access to customer data are restricted through the use of unique user account IDs. Access to sensitive systems and applications requires two-factor authentication in the form of unique user IDs, strong passwords, security keys, and/or certificates. Periodic reviews of access lists help ensure that access to customer data (and other need-to-know data) is appropriate and authorized. Access to production machines, network devices, and support tools is managed via an access group management system. Membership in these groups must be approved by respective group administrators. User group memberships are reviewed semiannually under the direction of the group administrators to ensure that access has been removed for employees who no longer have a business need for such access.

Access authorization in Apigee Edge is enforced at all relevant layers of the system. The granting or modification of access rights is based on the user's job responsibilities or on a need-to-know basis and must be authorized and approved by the user's functional manager or system owners. Approvals are managed by workflow tools and logged. Production system access is granted only to individuals who have completed the required security and privacy training and require this level of access to perform required tasks. Access to all corporate and production resources is automatically removed upon submission of a termination request by the manager of any departing employee, or by the appropriate Human Resources manager.

Password Guidelines

Google personnel are required to authenticate using valid credentials prior to resetting their password. Passwords are managed in accordance with a set of password construction, protection, and management guidelines, which enforce the following:

- Minimum length
- Complexity
- History
- Idle time lockout setting

Password configuration requirements are enforced by internal systems. In addition to the security requirements enforced during configuration, internal passwords are subject to cryptographic hashing to mitigate the risk of unauthorized disclosure or modification.

Google has supplemented passwords with a two-factor authentication requirement for internal personnel to access sensitive internal corporate and production services and to access Apigee Edge in the production environment from the corporate network. Two-factor authentication provides additional protection to prevent user account manipulation in case the user's password is compromised.

Change Management

Changes to Apigee Edge are delivered as software releases. Change management policies, including security code reviews and emergency fixes, are in place, and procedures for tracking, testing, approving, and validating changes are documented. Each service has a documented release process that specifies the procedures to be used, including definitions of the scope of changes to be delivered, source code control, code review, building, testing, and record keeping.

The change process starts with a developer checking out source code files from the source control system to modify them. Once development is complete, the developer performs unit testing, if applicable. A peer reviews the changes before the code is checked back into the source control system. The Company requires that a code reviewer be independent of the assigned developer and follow coding standards. Once the changes to be delivered are complete, the release process begins. The launch engineer reviews the results of the service's continuous build and test system and chooses a change version at which the build and tests all succeed. The needed components for this change version are then migrated to a release branch. The programs to be released are compiled from a source taken from the release branch.

The compiled binary is tested in a quality assurance environment or by pushing a canary. A canary is a not-yet-released binary that is migrated into a production system in a limited and controlled way. Once quality assurance and developers agree that the binary is satisfactory, the release is finalized and deployed to production using a release tool.

Tools are also utilized to detect deviations from pre-defined OS configurations on production machines and to correct them automatically. This allows for an easy rollout of updates to system files in a consistent manner and helps ensure that machines are automatically updated.

Vulnerability Management

The goal of Google's vulnerability management program is to investigate and respond to all relevant security vulnerabilities. The vulnerability management guidelines describe how vulnerabilities are detected, classified, and remediated. As part of this program, the Security Operations team conducts network vulnerability scans to detect vulnerabilities in software, systems, and network devices. These scans are conducted using an approved security vendor quarterly and after any significant changes in the network.

External independent third-party penetration tests are performed annually for a pre-determined subset of the services included in Apigee Edge, and corrective actions are taken, as necessary. The subset of services included in any given year is determined by the Security and engineering compliance teams and based on their understanding of the organization's current risk environment, as well as the organization's current regulatory and compliance requirements.

Incident Management

Dedicated on-call personnel, incident response teams, and customer support technicians are responsible for performing incident management services, and they also initiate, manage, respond to, and track incidents. The team is organized into formalized shifts and includes individuals designated as on-call personnel.

Google has established a dedicated security team responsible for managing security and helping to resolve emergencies 24/7 worldwide. Incident response policies are in place, and procedures for resolving critical incidents are documented.

Incident Alert and Recording

Incident alerts are initiated whenever an incident occurs. In response to an alert, production monitoring tools automatically generate notifications for the incident management team when a monitored threshold is exceeded. A ticket may also be manually created by an employee when an issue is identified or in response to a customer service request. The monitoring systems have the ability to send well-formed alert messages to a separate alert manager tool. The alert manager tool combines alerts from various sources and handles policies for contacting users in a sensible manner. It also provides a dashboard view of all the monitoring processes.

An incident ticket may be created concurrently depending on the type of incident. The incident ticket is designed to capture information necessary for incident and problem resolution (e.g., origin, service description, impacted area). The incident ticket continues to be populated as it is worked from initiation through resolution and may be linked to a root cause analysis or resolution requirements. After defining the impact of the incident and the recurrence probability, the incident ticket is assigned a severity level to prioritize its importance and direct resources to those incidents of greatest impact. Each severity level has been formally defined to capture the importance of each incident or problem type.

Incident Escalation

The Company has documented escalation procedures and communication protocols that address incident handling and the notification of appropriate individuals. Escalated issues are treated in the same manner as monitoring alerts by the on-call staff. The burden of proof is on the on-call engineer to demonstrate that the problem is not in their area.

Alert escalation is performed by an internal escalation tool and based on acknowledgements. The monitoring tools are integrated with the alert manager tool and communicate with the escalation tool via email. The escalation time and contacts are defined in the escalation tool configuration files. If the tool does not receive an acknowledgement from the paged contacts, automated escalation occurs.

Incident Resolution

After gathering the necessary information about the incident, the incident ticket is assigned to the appropriate support area based on the nature of the problem or the root cause. If the incident exists in another environment or is a recurring problem, the incident ticket is flagged for further investigation after resolution. Incidents are usually forwarded to one of the corresponding technical departments: system reliability engineers and software engineers, database administrators (DBAs), systems administrators, application administrators, network security, and platform support.

The incident ticket is closed upon resolution of the incident. Google also has an established process for notifying customers of data security incidents that affect their accounts.

Data Retention and Deletion

Google has procedures in place to dispose of confidential information according to Google's data retention and deletion policy. Google maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers. Data media destruction is done internally or by a certified third-party supplier.

Backup and Recovery

A multi-location strategy for production environments is employed to permit the resumption of operations at other GCP and AWS regions in the event of the loss of a region. These locations are connected through multiple encrypted network links and interfaces. This provides high availability by dynamically load balancing across those sites. Google uses a dashboard that provides details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource parameters.

Disaster Recovery

To minimize service interruption due to system failure, natural disaster, or other catastrophes, Google designs its infrastructure and services to be resilient to software, hardware, or facilities failures. Redundant architecture is in place to distribute resources across geographically dispersed locations to support continuous availability. High-speed connections between the locations help ensure swift failover.

The disaster recovery program enables disaster readiness, response, and recovery of Google's business, systems, and data. Google conducts disaster recovery testing annually to provide a coordinated venue for infrastructure and application teams to test communication plans, fail-over scenarios, operational transitions, and other emergency responses. All teams that participate in the disaster recovery exercise develop testing plans and postmortems that document the results and lessons learned from the tests.

Monitoring

Management performs monitoring activities continuously to assess the quality of internal control over time. This involves assessing the design and operation of controls and taking necessary corrective actions.

Monitoring activities are used to initiate corrective action through department meetings and informal notifications. Management is responsible for directing and controlling operations and for establishing, communicating, and monitoring control activities and procedures.

Management emphasizes maintaining sound internal controls, as well as communicating integrity and ethical values to personnel. This is accomplished through ongoing activities, separate evaluations, or a combination of the two. Monitoring activities include using information from communications from external parties, such as user entity complaints and regulatory comments, which may indicate problems or highlight areas in need of improvement. Management has implemented a self-assessment and compliance program to ensure that the controls are consistently applied as designed.

Ongoing Monitoring

The control environment and control effectiveness are informally and continuously evaluated. The information security officer is responsible for the maintenance and monitoring of ongoing security activities.

Examples of Google's ongoing monitoring activities include the following:

- Management obtains evidence that the system of internal control continues to function as part of its regular management activities.
- Organizational structure and supervisory activities provide oversight of control functions and identification of deficiencies.
- Management continuously evaluates existing policies and develops new policies when necessary for monitoring the control environment.
- Personnel are briefed on organizational policy statements and codes of conduct to communicate entity values.
- Apigee Edge is monitored continuously using automated alerting tools.
- Management holds all-hands meetings as needed to communicate organizational results and objectives.

Separate Evaluations

The evaluation of an entire internal control system may be prompted by several reasons, including major strategy or management changes, major acquisitions or dispositions, or significant changes in operations or methods of processing information. Management has implemented a self-assessment program to evaluate the performance of specific control activities and processes over time and to confirm that the in-scope controls were consistently applied as designed, including whether manual controls were applied by individuals who have the competence and authority to do so. Evaluations of internal control vary in scope and frequency depending on the significance of risks being controlled and the importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often.

Evaluations often take the form of self-assessments, in which personnel responsible for a particular unit or function determine the effectiveness of controls for their activities. These assessments are considered by management, along with any other internal control evaluations. The findings of these efforts are utilized to ensure that follow-up actions are taken, and subsequent evaluations are modified, as necessary. Departmental evaluations occur regularly as dictated by Company objectives. These evaluations document the assessment of the department and any process-level improvements that would help achieve Google's Company-wide goals. Any identified areas for improvement that could inhibit the effectiveness of the control environment are immediately discussed, analyzed, and implemented by the operations team where applicable.

Complementary User Entity Controls (CUECs)

Google's controls related to Apigee Edge cover only a portion of overall internal control for each user entity of Apigee Edge. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls and the related tests and results described in Section 4 of this report, taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames. • Controls to provide reasonable assurance that the Company is notified of changes in: – User entity vendor security requirements – The authorized users list
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: – Inform their employees and users that their information or data is being used and stored by the Company. – Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
CC6.1	• User entities grant access to the Company's system to authorized and trained personnel.
CC6.4 CC7.2 A1.2	• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.
CC6.6	• Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses GCP and AWS as subservice organizations for IaaS services. The Company's controls related to Apigee Edge cover only a portion of the overall internal control for each user entity of Apigee Edge. The description does not extend to the IaaS services for IT infrastructure provided by the subservice organizations. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of GCP and AWS.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at GCP and AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. GCP and AWS' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. GCP and AWS' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the GCP and AWS SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by GCP and AWS to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to GCP and AWS management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to Apigee Edge to be achieved solely by Google. Therefore, each user entity's internal control must be evaluated in

conjunction with Google's controls and related tests and results described in Section 4 of this report, taking into account the related CSOCs expected to be implemented at GCP and AWS as described below.

Criteria	Complementary Subservice Organization Controls
CC6.4	• GCP and AWS are responsible for restricting data center access to authorized personnel. • GCP and AWS are responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5 CC6.7	• GCP and AWS are responsible for establishing procedures to remove data and software stored on hosted equipment and to render such data and software unreadable.
CC7.2 A1.2	• GCP and AWS are responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • GCP and AWS are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • GCP and AWS are responsible for overseeing the regular maintenance of environmental protections at data centers.

Specific Criteria Not Relevant to the System

There were no specific security, availability, or confidentiality Trust Services Criteria as set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC) that were not relevant to the system as presented in this report.

Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how Apigee Edge was used to provide the service from April 1, 2022 to March 31, 2023.

Report Use

The description does not omit or distort information relevant to Apigee Edge while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to their own particular needs.

Section 4

Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories

Control Environment Elements

The control environment represents the collective effect of various elements in establishing, enhancing or mitigating the effectiveness of specific controls. The control environment elements as described in the description of the system include, but are not limited to, the Code of Conduct, Policies and Procedures and Human Resources.

Our tests of the control environment included the following procedures, to the extent we considered necessary; (a) an inspection of Google's organizational structure including segregation of functional responsibilities and policies and procedures; (b) inquiries with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls; (c) observations of personnel in the performance of their assigned duties; and (d) inspection of documents and records pertaining to controls.

Description of Tests Performed by Coalfire Controls, LLC

Our tests of operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the trust services security, availability, and confidentiality categories and criteria were achieved throughout the period April 1, 2022 to March 31, 2023. In selecting particular tests of the operating effectiveness of the controls, we considered (i) the nature of the controls being tested; (ii) the types of available evidential matter; (iii) the nature of the criteria to be achieved; (iv) the assessed level of control risk; and (v) the expected efficiency and effectiveness of the test. Such tests were used to evaluate fairness of the presentation of the description of Google's Apigee Edge API Management Platform and to evaluate the operating effectiveness of specified controls.

Additionally, observation and inspection procedures were performed as it relates to system generated reports, queries, and listings within management's description of the system to assess the completeness and accuracy (reliability) of the information utilized in the performance of our testing of the control activities.

Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, and Confidentiality Categories

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC1.1	The entity demonstrates a commitment to integrity and ethical values.		
	The Company has established internal privacy and information security policies, as well as a Code of Conduct.	Inspected the Code of Conduct, Basic Internal Privacy Policy, Information Security Policy, Data Security Policy, and Security and Resilience Policy to determine that the Company had established internal privacy and information security policies, as well as a Code of Conduct.	No exceptions noted.
	Employees of the Company are required to acknowledge the Code of Conduct and information security policies upon hire.	Inspected acknowledgements of the Code of Conduct and information security policies for a sample of new hires to determine that employees were required to acknowledge the Code of Conduct and information security policies upon hire.	No exceptions noted.
	The Company has established and enforces a disciplinary process to address non-compliance with Company policies, the Code of Conduct, or other personnel requirements.	Inspected the Code of Conduct to determine that the Company had established a disciplinary process to address non-compliance with Company policies, the Code of Conduct, or other personnel requirements.	No exceptions noted.
		Inspected disciplinary case records for a sample of disciplinary incidents to determine that the Company had enforced a disciplinary process to address non-compliance with Company policies, the Code of Conduct, or other personnel requirements.	No exceptions noted.
	Background checks are required to be performed on new hires, as permitted by local laws, upon hire.	Inspected the guidelines for the hiring process to determine that background checks were required to be performed on new hires, as permitted by local laws, upon hire.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected background check completion evidence for a sample of new hires to determine that background checks were performed on new hires, as permitted by local laws, upon hire.	No exceptions noted.
	The Company establishes confidentiality agreements with employees and extended workforce personnel to define responsibilities and expected behavior for the protection of information.	Inspected employees and extended workforce personnel responsibilities and expected behavior for the protection of information within the confidentiality agreement template to determine that the Company established confidentiality agreements with employees and extended workforce personnel to define responsibilities and expected behavior for the protection of information.	No exceptions noted.
		Inspected confidentiality agreement acknowledgements for a sample of employees and extended workforce personnel to determine that employees and extended workforce personnel acknowledged the Company's established confidentiality agreements that defined responsibilities and expected behavior for the protection of information.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
	The board of directors demonstrates independence from management, exercises oversight of the development and performance of internal control, and meets at least annually.	Inspected the board's documented oversight responsibilities relative to internal control within the Corporate Governance Guidelines and an example board meeting calendar invite and agenda topics to determine that the board of directors exercised oversight of the development and performance of internal control and met at least annually.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected a listing of the board of directors on the Investor Relations webpage to determine that the board demonstrated independence from management.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
	The Company has implemented a formal reporting structure that is made available to personnel.	Inspected organizational charts and the functional reporting structure made available to personnel on the Company's intranet to determine that the Company had implemented a formal reporting structure that was made available to personnel.	No exceptions noted.
	The board of directors demonstrates independence from management, exercises oversight of the development and performance of internal control, and meets at least annually.	Inspected the board's documented oversight responsibilities relative to internal control within the Corporate Governance Guidelines and an example board meeting calendar invite and agenda topics to determine that the board of directors exercised oversight of the development and performance of internal control and met at least annually.	No exceptions noted.
		Inspected a listing of the board of directors on the Investor Relations webpage to determine that the board demonstrated independence from management.	No exceptions noted.
	Company goals and responsibilities are required to be developed and communicated by management at least annually and amended as needed. Results are evaluated and communicated to employees.	Inspected the management review of the Information Security Management System (ISMS) report, the Company's Objectives and Key Results (OKR) documentation, and Company newsletters to determine that Company goals and responsibilities were required to be developed and communicated by management at least annually and amended as needed and that results were evaluated and communicated to employees.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Information security and privacy is managed by an executive who is dedicated to Security and Privacy, is independent of IT responsibility, and may escalate to the board level concerning security issues.	Inspected the Security and Privacy organizational charts on the Company's intranet to determine that information security and privacy was managed by an executive who was dedicated to Security and Privacy, was independent of IT responsibility, and had the ability to escalate security issues to the board level if necessary.	No exceptions noted.
		Inspected an example calendar invite and meeting agenda for a recent Security and Privacy team meeting to determine that a Security and Privacy executive met with relevant personnel to discuss security issues and was able to escalate security issues to the board level as necessary.	No exceptions noted.
	New hires and internal transfers are required to go through an official recruiting process, during which they are screened against detailed job descriptions and interviewed to assess competence.	Inspected onboarding records and job descriptions for a sample of new hires and internal transfers to determine that new hires and internal transfers were required to go through an official recruiting process, during which they were screened against detailed job descriptions and interviewed to assess competence.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
	The Company has established a privacy and information security training program and requires relevant personnel to complete this training annually.	Inspected the internal Privacy Policy, privacy and information security training program materials, and compliance monitoring tools to determine that a privacy and information security training program was established and relevant personnel were required to complete this training annually.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the compliance monitoring tool dashboard used by management to monitor the completion rate for employees' completion of the required privacy and information security training, as well as an example of an email notification sent to employees for overdue training, to determine that the Company had established a privacy and information security training program and that relevant personnel met the requirement to complete the training annually.	No exceptions noted.
	New hires and internal transfers are required to go through an official recruiting process, during which they are screened against detailed job descriptions and interviewed to assess competence.	Inspected onboarding records and job descriptions for a sample of new hires and internal transfers to determine that new hires and internal transfers were required to go through an official recruiting process, during which they were screened against detailed job descriptions and interviewed to assess competence.	No exceptions noted.
	Background checks are required to be performed on new hires, as permitted by local laws, upon hire.	Inspected the guidelines for the hiring process to determine that background checks were required to be performed on new hires, as permitted by local laws, upon hire.	No exceptions noted.
		Inspected background check completion evidence for a sample of new hires to determine that background checks were performed on new hires, as permitted by local laws, upon hire.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
	The Company has established internal privacy and information security policies, as well as a Code of Conduct.	Inspected the Code of Conduct, Basic Internal Privacy Policy, Information Security Policy, Data Security Policy, and Security and Resilience Policy to determine that the Company had established internal privacy and information security policies, as well as a Code of Conduct.	No exceptions noted.
	Employees of the Company are required to acknowledge the Code of Conduct and information security policies upon hire.	Inspected acknowledgements of the Code of Conduct and information security policies for a sample of new hires to determine that employees were required to acknowledge the Code of Conduct and information security policies upon hire.	No exceptions noted.
	The Company has established and enforces a disciplinary process to address non-compliance with Company policies, the Code of Conduct, or other personnel requirements.	Inspected the Code of Conduct to determine that the Company had established a disciplinary process to address non-compliance with Company policies, the Code of Conduct, or other personnel requirements.	No exceptions noted.
		Inspected disciplinary case records for a sample of disciplinary incidents to determine that the Company had enforced a disciplinary process to address non-compliance with Company policies, the Code of Conduct, or other personnel requirements.	No exceptions noted.
	New hires and internal transfers are required to go through an official recruiting process, during which they are screened against detailed job descriptions and interviewed to assess competence.	Inspected onboarding records and job descriptions for a sample of new hires and internal transfers to determine that new hires and internal transfers were required to go through an official recruiting process, during which they were screened against detailed job descriptions and interviewed to assess competence.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Information security and privacy is managed by an executive who is dedicated to Security and Privacy, is independent of IT responsibility, and may escalate to the board level concerning security issues.	Inspected the Security and Privacy organizational charts on the Company's intranet to determine that information security and privacy was managed by an executive who was dedicated to Security and Privacy, was independent of IT responsibility, and had the ability to escalate security issues to the board level if necessary.	No exceptions noted.
		Inspected an example calendar invite and meeting agenda for a recent Security and Privacy team meeting to determine that a Security and Privacy executive met with relevant personnel to discuss security issues and was able to escalate security issues to the board level as necessary.	No exceptions noted.
	Company goals and responsibilities are required to be developed and communicated by management at least annually and amended as needed. Results are evaluated and communicated to employees.	Inspected the management review of the Information Security Management System (ISMS) report, the Company's Objectives and Key Results (OKR) documentation, and Company newsletters to determine that Company goals and responsibilities were required to be developed and communicated by management at least annually and amended as needed and that results were evaluated and communicated to employees.	No exceptions noted.
	Management performs assessments of internal identity, authentication, and source code management controls at least annually. Corrective actions are taken based on relevant findings.	Inspected tickets and documentation of the Company's organizational risk assessment evaluations to determine that management performed assessments of internal identity, authentication, and source code management controls at least annually and that corrective actions were taken based on relevant findings.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
	The Company has an established Internal Audit function that evaluates management's compliance with security controls annually.	Inspected the Internal Audit report to determine that the Company had an established Internal Audit function that evaluated management's compliance with security controls annually.	No exceptions noted.
	Management performs assessments of internal identity, authentication, and source code management controls at least annually. Corrective actions are taken based on relevant findings.	Inspected tickets and documentation of the Company's organizational risk assessment evaluations to determine that management performed assessments of internal identity, authentication, and source code management controls at least annually and that corrective actions were taken based on relevant findings.	No exceptions noted.
	The Company has implemented a vulnerability management program to detect and remediate system vulnerabilities. Remediation plans are developed, implemented, and tracked through remediation or to resolution for, at a minimum, all critical and high security deficiencies and are tracked within internal tools.	Inspected the Vulnerability Management Guidelines and the Vulnerability Priority Guidelines available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect and remediate system vulnerabilities and that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.
		Inspected tickets for a sample of security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools through remediation or to resolution for all critical and high security deficiencies identified during vulnerability detection activities.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Inspected the Log Data Usage Rules, the Security Logging Policy, the Vulnerability Management Policy, and the System Management Software Security Policy on the Company intranet to determine that the Company provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	No exceptions noted.
		Inspected monitoring tool dashboards, alerting configurations, and example alerts to determine that the Company provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	No exceptions noted.
	Audit logs are required to be continuously monitored for events related to security, confidentiality, and availability threats. Alerts are generated for further investigation.	Inspected the Information Security and Privacy Incident Response Policy to determine that audit logs were required to be continuously monitored for events related to security, availability, and confidentiality threats and that alerts were required to be generated for further investigation.	No exceptions noted.
		Inspected audit log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
		Inspected monitoring tool dashboards, alert threshold configurations, and examples alerts for events to determine that alerts were generated for further investigation.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
	The Company has established a privacy and information security training program and requires relevant personnel to complete this training annually.	Inspected the internal Privacy Policy, privacy and information security training program materials, and compliance monitoring tools to determine that a privacy and information security training program was established and relevant personnel were required to complete this training annually.	No exceptions noted.
		Inspected the compliance monitoring tool dashboard used by management to monitor the completion rate for employees' completion of the required privacy and information security training, as well as an example of an email notification sent to employees for overdue training, to determine that the Company had established a privacy and information security training program and that relevant personnel met the requirement to complete the training annually.	No exceptions noted.
	Information security and privacy is managed by an executive who is dedicated to Security and Privacy, is independent of IT responsibility, and may escalate to the board level concerning security issues.	Inspected the Security and Privacy organizational charts on the Company's intranet to determine that information security and privacy was managed by an executive who was dedicated to Security and Privacy, was independent of IT responsibility, and had the ability to escalate security issues to the board level if necessary.	No exceptions noted.
		Inspected an example calendar invite and meeting agenda for a recent Security and Privacy team meeting to determine that a Security and Privacy executive met with relevant personnel to discuss security issues and was able to escalate security issues to the board level as necessary.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	New hires and internal transfers are required to go through an official recruiting process, during which they are screened against detailed job descriptions and interviewed to assess competence.	Inspected onboarding records and job descriptions for a sample of new hires and internal transfers to determine that new hires and internal transfers were required to go through an official recruiting process, during which they were screened against detailed job descriptions and interviewed to assess competence.	No exceptions noted.
	The Company establishes security policies and procedures that clearly define information security responsibilities for all employees. Within the information security policies and procedures, the Company assigns responsibilities to the Information Security team. The Company manages operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of products and services.	Inspected the Company's security policies and procedures to determine that the Company defined information security responsibilities for all employees, delegated decisions on risk identification and resource prioritization to various engineering groups, and assigned responsibilities to the Information Security team.	No exceptions noted.
		Inspected the risk assessment to determine that the Company managed operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly supported the operation of the Company's products and services.	No exceptions noted.
	Changes to customer-facing services that may affect security, confidentiality, and availability are communicated to relevant personnel and impacted customers.	Inspected alert notifications and change ticket communication history for a sample of changes to customer-facing services to determine that relevant personnel were notified of changes to customer-facing services that could have affected security, confidentiality, and availability.	No exceptions noted.
		Inspected official product blogs, public community support pages, the issue tracker webpage, and the customer-facing log of vulnerabilities to determine that impacted customers were notified of changes to customer-facing services that could have affected security, confidentiality, and availability.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The descriptions of the Company's systems (including their scope and boundaries) are made available to internal teams.	Inspected the Apigee Edge system description within the Apigee Edge product site on the Company's intranet to determine that the descriptions of the Company's systems (including their scope and boundaries) were made available to internal teams.	No exceptions noted.
	The Company's security, confidentiality, and availability obligations for all employees are made available to internal teams.	Inspected the security policies and guidelines on the Company intranet to determine that they described security, confidentiality, and availability obligations for all employees and were made available to internal teams.	No exceptions noted.
	The Company has policies addressing security, confidentiality, and availability that have been approved by management and communicated to employees and are in accordance with ISO 27001.	Inspected the Company's security policies and procedures to determine that they addressed security, confidentiality, and availability and had been approved by management and were in accordance with ISO 27001.	No exceptions noted.
		Inspected the Company intranet accessible to all employees to determine that the Company had policies addressing security, confidentiality, and availability that had been communicated to employees.	No exceptions noted.
	Company goals and responsibilities are required to be developed and communicated by management at least annually and amended as needed. Results are evaluated and communicated to employees.	Inspected the management review of the Information Security Management System (ISMS) report, the Company's Objectives and Key Results (OKR) documentation, and Company newsletters to determine that Company goals and responsibilities were required to be developed and communicated by management at least annually and amended as needed and that results were evaluated and communicated to employees.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company has an established incident response policy that outlines management's responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the documented procedures for classification, prioritization, consolidation, and escalation of security incidents per criticality within the Information Security and Privacy Incident Response Policy to determine that the Company had established a documented incident response policy that outlined management's responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.
		Inspected security event tickets, post-mortem documentation, and customer communications for a sample of security events to determine that management implemented procedures to ensure quick, effective, and orderly responses to information security incidents.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		
	The Company's commitments to security, availability, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS) and the Data Processing and Security Terms (DPST).	Inspected the ToS to determine that the Company's commitments to security, availability, and confidentiality were communicated to external users via publications such as the ToS.	No exceptions noted.
		Inspected the Data Processing and Security Terms (DPST) to determine that the Company's commitments to security, availability, and confidentiality were communicated to users via publications.	No exceptions noted.
	The Company establishes agreements, including non-disclosure agreements (NDAs), for preserving confidentiality of information and software exchanges with external parties.	Inspected the NDA templates to determine that the Company's agreements, including NDAs, provided details on preserving confidentiality of information and software exchanges.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected NDA acknowledgements for a sample of external parties to determine that the Company established agreements, including NDAs, for preserving confidentiality of information and software exchanges with external parties.	No exceptions noted.
	The Company has implemented an addendum to contract with processors (including sub-processors). The addendum defines the security obligations that the processor must meet to satisfy the Company's obligations regarding customer data.	Inspected the DPST template to determine that the DPST contained an addendum that defined the security obligations that processors (including sub-processors) had to meet to satisfy the Company's obligations regarding customer data.	No exceptions noted.
		Inspected the Inbound Service Agreement (ISA) and the Subprocessor Data Processing Agreement (SDPA) for a sample of processors and sub-processors supporting the in-scope systems to determine that the Company had implemented an addendum to contract with processors and sub-processors.	No exceptions noted.
		Inspected the termination clause for service or product issues related to vendors within an example ISA to determine that it defined the security obligations that processors (including sub-processors) had to meet to satisfy the Company's obligations regarding customer data.	No exceptions noted.
	The Company takes a risk-based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessments as determined by the sensitivity of data being processed or access being granted.	Inspected the Vendor Security Assessment Guidelines to determine that the Company had a documented, risk-based approach to reviewing the security practices of vendors and the security posture of vendor products.	No exceptions noted.
		Inspected the Vendor Security Audit review documentation for a sample of vendors to determine that the reviews included automated and manual assessments as determined by the sensitivity of data being processed or access being granted.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Changes to customer-facing services that may affect security, confidentiality, and availability are communicated to relevant personnel and impacted customers.	Inspected alert notifications and change ticket communication history for a sample of changes to customer-facing services to determine that relevant personnel were notified of changes to customer-facing services that could have affected security, confidentiality, and availability.	No exceptions noted.
		Inspected official product blogs, public community support pages, the issue tracker webpage, and the customer-facing log of vulnerabilities to determine that impacted customers were notified of changes to customer-facing services that could have affected security, confidentiality, and availability.	No exceptions noted.
	The Company provides external users with mechanisms to report security issues, incidents, and concerns.	Inspected Google support documentation and external support resources to determine that the Company provided external users with mechanisms to report security issues, incidents, and concerns.	No exceptions noted.
	Descriptions of the Company's system and its boundaries are available to authorized external users via ongoing communications with customers or via its official blog postings.	Inspected the Product Overview Guide page for Apigee within the Google Cloud site that was available to existing customers and the product blog to determine that descriptions of the Company's system and its boundaries were available to authorized external users via ongoing communications with customers or via its official blog postings.	No exceptions noted.
	Customer responsibilities are described on the Company's product websites or in system documentation.	Inspected customer responsibilities on product websites and in system documentation, as well as the ToS, that was accessible by internal and external customers to determine that customer responsibilities were described.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
	Company goals and responsibilities are required to be developed and communicated by management at least annually and amended as needed. Results are evaluated and communicated to employees.	Inspected the management review of the Information Security Management System (ISMS) report, the Company's Objectives and Key Results (OKR) documentation, and Company newsletters to determine that Company goals and responsibilities were required to be developed and communicated by management at least annually and amended as needed and that results were evaluated and communicated to employees.	No exceptions noted.
	The Company develops and maintains a risk management framework to manage risk to an acceptable level. Company management evaluates risks by defining risk ratings and considers the risk of engaging with third parties.	Inspected the risk management guidelines to determine that the Company developed and maintained a risk management framework to manage risk to an acceptable level.	No exceptions noted.
		Inspected risk management guidelines and the risk assessment documentation to determine that Company management evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	No exceptions noted.
	The Company conducts annual Information Security Risk Assessments to identify and evaluate risks, and the Company's operational objectives and potential impacts and changes to the Company business model are considered. This risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment performed for in-scope systems to determine that the Company conducted an Information Security Risk Assessment to identify and evaluate risks during the period.	No exceptions noted.
		Inspected the risk assessment to determine that the risk assessment considered the Company's operational objectives, potential impacts and changes to the Company business model, and the potential for fraud and how fraud could have impacted the achievement of objectives.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the Insider Risk website to determine that the Company considered the potential for fraud and how fraud could have impacted the achievement of objectives within the risk assessment.	No exceptions noted.
	As part of the annual risk assessment, risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented, and approved by management.	Inspected the annual risk assessment and tickets to determine that, as part of the annual risk assessment, risks were mitigated to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
	The Company develops and maintains a risk management framework to manage risk to an acceptable level. Company management evaluates risks by defining risk ratings and considers the risk of engaging with third parties.	Inspected the risk management guidelines to determine that the Company developed and maintained a risk management framework to manage risk to an acceptable level.	No exceptions noted.
		Inspected risk management guidelines and the risk assessment documentation to determine that Company management evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	No exceptions noted.
	The Company conducts annual Information Security Risk Assessments to identify and evaluate risks, and the Company's operational objectives and potential impacts and changes to the Company business model are considered. This risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment performed for in-scope systems to determine that the Company conducted an Information Security Risk Assessment to identify and evaluate risks during the period.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the risk assessment to determine that the risk assessment considered the Company's operational objectives, potential impacts and changes to the Company business model, and the potential for fraud and how fraud could have impacted the achievement of objectives.	No exceptions noted.
		Inspected the Insider Risk website to determine that the Company considered the potential for fraud and how fraud could have impacted the achievement of objectives within the risk assessment.	No exceptions noted.
	As part of the annual risk assessment, risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented, and approved by management.	Inspected the annual risk assessment and tickets to determine that, as part of the annual risk assessment, risks were mitigated to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No exceptions noted.
	The Company has geographically dispersed personnel from Security Incident Response Teams who are responsible for managing information security incidents and the investigations and dispositions of information security incidents.	Inspected internal incident response websites and the process in place for Security Incident Response Teams to quantify and monitor incidents within the Information Security and Privacy Incident Response Policy to determine that the Company had geographically dispersed personnel from Security Incident Response Teams who were responsible for the management of information security incidents and the investigations and dispositions of information security incidents.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company conducts disaster recovery (DR) and business continuity (BC) testing continuously (and requires it to be conducted at least annually) to enable infrastructure and application teams to test communication plans, failover scenarios, operational transitions, and other emergency responses. Participating teams create testing plans and document the results and lessons learned from the tests.	Inspected the DR and BC planning documentation, testing checklist, and testing results to determine that DR and BC testing was conducted by the infrastructure and application teams at least annually and that testing included communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.
		Inspected DR and BC testing documentation to determine that participating teams created testing plans and documented the results and lessons learned from the tests.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
	The Company develops and maintains a risk management framework to manage risk to an acceptable level. Company management evaluates risks by defining risk ratings and considers the risk of engaging with third parties.	Inspected the risk management guidelines to determine that the Company developed and maintained a risk management framework to manage risk to an acceptable level.	No exceptions noted.
		Inspected risk management guidelines and the risk assessment documentation to determine that Company management evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	No exceptions noted.
	The Company conducts annual Information Security Risk Assessments to identify and evaluate risks, and the Company's operational objectives and potential impacts and changes to the Company business model are considered. This risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment performed for in-scope systems to determine that the Company conducted an Information Security Risk Assessment to identify and evaluate risks during the period.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the risk assessment to determine that the risk assessment considered the Company's operational objectives, potential impacts and changes to the Company business model, and the potential for fraud and how fraud could have impacted the achievement of objectives.	No exceptions noted.
		Inspected the Insider Risk website to determine that the Company considered the potential for fraud and how fraud could have impacted the achievement of objectives within the risk assessment.	No exceptions noted.
	As part of the annual risk assessment, risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented, and approved by management.	Inspected the annual risk assessment and tickets to determine that, as part of the annual risk assessment, risks were mitigated to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
	Penetration tests are performed at least annually.	Inquired of management and inspected the annual penetration test to determine that penetration tests were performed at least annually.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all high and medium vulnerabilities identified during the annual penetration test.	Inspected remediation plans for vulnerabilities identified during the penetration test to determine that a remediation plan was developed and changes were implemented to remediate, at a minimum, all high and medium vulnerabilities identified during the annual penetration test.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company develops and maintains a risk management framework to manage risk to an acceptable level. Company management evaluates risks by defining risk ratings and considers the risk of engaging with third parties.	Inspected the risk management guidelines to determine that the Company developed and maintained a risk management framework to manage risk to an acceptable level.	No exceptions noted.
		Inspected risk management guidelines and the risk assessment documentation to determine that Company management evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	No exceptions noted.
	The Company conducts annual Information Security Risk Assessments to identify and evaluate risks, and the Company's operational objectives and potential impacts and changes to the Company business model are considered. This risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment performed for in-scope systems to determine that the Company conducted an Information Security Risk Assessment to identify and evaluate risks during the period.	No exceptions noted.
		Inspected the risk assessment to determine that the risk assessment considered the Company's operational objectives, potential impacts and changes to the Company business model, and the potential for fraud and how fraud could have impacted the achievement of objectives.	No exceptions noted.
		Inspected the Insider Risk website to determine that the Company considered the potential for fraud and how fraud could have impacted the achievement of objectives within the risk assessment.	No exceptions noted.
	As part of the annual risk assessment, risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented, and approved by management.	Inspected the annual risk assessment and tickets to determine that, as part of the annual risk assessment, risks were mitigated to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company has implemented a vulnerability management program to detect and remediate system vulnerabilities. Remediation plans are developed, implemented, and tracked through remediation or to resolution for, at a minimum, all critical and high security deficiencies and are tracked within internal tools.	Inspected the Vulnerability Management Guidelines and the Vulnerability Priority Guidelines available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect and remediate system vulnerabilities and that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.
		Inspected tickets for a sample of security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools through remediation or to resolution for all critical and high security deficiencies identified during vulnerability detection activities.	No exceptions noted.

Monitoring Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
	The Company has an established Internal Audit function that evaluates management's compliance with security controls annually.	Inspected the Internal Audit report to determine that the Company had an established Internal Audit function that evaluated management's compliance with security controls annually.	No exceptions noted.
	Penetration tests are performed at least annually.	Inquired of management and inspected the annual penetration test to determine that penetration tests were performed at least annually.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all high and medium vulnerabilities identified during the annual penetration test.	Inspected remediation plans for vulnerabilities identified during the penetration test to determine that a remediation plan was developed and changes were implemented to remediate, at a minimum, all high and medium vulnerabilities identified during the annual penetration test.	No exceptions noted.
	The Company takes a risk-based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessments as determined by the sensitivity of data being processed or access being granted.	Inspected the Vendor Security Assessment Guidelines to determine that the Company had a documented, risk-based approach to reviewing the security practices of vendors and the security posture of vendor products.	No exceptions noted.
		Inspected the Vendor Security Audit review documentation for a sample of vendors to determine that the reviews included automated and manual assessments as determined by the sensitivity of data being processed or access being granted.	No exceptions noted.

Monitoring Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Management performs assessments of internal identity, authentication, and source code management controls at least annually. Corrective actions are taken based on relevant findings.	Inspected tickets and documentation of the Company's organizational risk assessment evaluations to determine that management performed assessments of internal identity, authentication, and source code management controls at least annually and that corrective actions were taken based on relevant findings.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
	The Company has an established Internal Audit function that evaluates management's compliance with security controls annually.	Inspected the Internal Audit report to determine that the Company had an established Internal Audit function that evaluated management's compliance with security controls annually.	No exceptions noted.
	The Company takes a risk-based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessments as determined by the sensitivity of data being processed or access being granted.	Inspected the Vendor Security Assessment Guidelines to determine that the Company had a documented, risk-based approach to reviewing the security practices of vendors and the security posture of vendor products.	No exceptions noted.
		Inspected the Vendor Security Audit review documentation for a sample of vendors to determine that the reviews included automated and manual assessments as determined by the sensitivity of data being processed or access being granted.	No exceptions noted.
	Management performs assessments of internal identity, authentication, and source code management controls at least annually. Corrective actions are taken based on relevant findings.	Inspected tickets and documentation of the Company's organizational risk assessment evaluations to determine that management performed assessments of internal identity, authentication, and source code management controls at least annually and that corrective actions were taken based on relevant findings.	No exceptions noted.

Monitoring Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company has implemented a vulnerability management program to detect and remediate system vulnerabilities. Remediation plans are developed, implemented, and tracked through remediation or to resolution for, at a minimum, all critical and high security deficiencies and are tracked within internal tools.	Inspected the Vulnerability Management Guidelines and the Vulnerability Priority Guidelines available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect and remediate system vulnerabilities and that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.
		Inspected tickets for a sample of security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools through remediation or to resolution for all critical and high security deficiencies identified during vulnerability detection activities.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
	The Company has an internal audit function and regularly engages third parties to conduct independent reviews of the effectiveness of the Company's approach to managing information security.	Inspected internal audit program manuals and compliance guidelines that required the independent audit of IT systems and components at least annually to determine that the Company had an internal audit function that regularly engaged with third parties to conduct independent reviews of the effectiveness of the Company's approach to managing information security.	No exceptions noted.
		Inspected the Company's security compliance certifications obtained through independent audits of IT systems and components to determine that the Company regularly engaged third parties to conduct independent reviews of the effectiveness of the Company's approach to managing information security.	No exceptions noted.
	As part of the annual risk assessment, risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented, and approved by management.	Inspected the annual risk assessment and tickets to determine that, as part of the annual risk assessment, risks were mitigated to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No exceptions noted.
	The Company develops and maintains a risk management framework to manage risk to an acceptable level. Company management evaluates risks by defining risk ratings and considers the risk of engaging with third parties.	Inspected the risk management guidelines to determine that the Company developed and maintained a risk management framework to manage risk to an acceptable level.	No exceptions noted.
		Inspected risk management guidelines and the risk assessment documentation to determine that Company management evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company conducts annual Information Security Risk Assessments to identify and evaluate risks, and the Company's operational objectives and potential impacts and changes to the Company business model are considered. This risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment performed for in-scope systems to determine that the Company conducted an Information Security Risk Assessment to identify and evaluate risks during the period.	No exceptions noted.
		Inspected the risk assessment to determine that the risk assessment considered the Company's operational objectives, potential impacts and changes to the Company business model, and the potential for fraud and how fraud could have impacted the achievement of objectives.	No exceptions noted.
		Inspected the Insider Risk website to determine that the Company considered the potential for fraud and how fraud could have impacted the achievement of objectives within the risk assessment.	No exceptions noted.
	The Company separates duties of individuals by granting users access based on job responsibilities and least privilege and by limiting access to only authorized users.	Inspected the Account Security Policy and the Identity and Access Management Policy to determine that the Company separated duties of individuals by granting users access based on job responsibilities and least privilege and by limiting access to only authorized users.	No exceptions noted.
		Observed an attempt to access a privileged system outside the realm of the user's job responsibilities to determine that the attempt to violate the separation of duties failed and that the Company separated duties and implemented a principle of least privilege by limiting access to only authorized users.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.		
	The Company develops and maintains a risk management framework to manage risk to an acceptable level. Company management evaluates risks by defining risk ratings and considers the risk of engaging with third parties.	Inspected the risk management guidelines to determine that the Company developed and maintained a risk management framework to manage risk to an acceptable level.	No exceptions noted.
		Inspected risk management guidelines and the risk assessment documentation to determine that Company management evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	No exceptions noted.
	The Company has an internal audit function and regularly engages third parties to conduct independent reviews of the effectiveness of the Company's approach to managing information security.	Inspected internal audit program manuals and compliance guidelines that required the independent audit of IT systems and components at least annually to determine that the Company had an internal audit function that regularly engaged with third parties to conduct independent reviews of the effectiveness of the Company's approach to managing information security.	No exceptions noted.
		Inspected the Company's security compliance certifications obtained through independent audits of IT systems and components to determine that the Company regularly engaged third parties to conduct independent reviews of the effectiveness of the Company's approach to managing information security.	No exceptions noted.
	As part of the annual risk assessment, risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented, and approved by management.	Inspected the annual risk assessment and tickets to determine that, as part of the annual risk assessment, risks were mitigated to acceptable levels based on risk criteria, including resolution time frames, which were established, documented, and approved by management.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company conducts annual Information Security Risk Assessments to identify and evaluate risks, and the Company's operational objectives and potential impacts and changes to the Company business model are considered. This risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment performed for in-scope systems to determine that the Company conducted an Information Security Risk Assessment to identify and evaluate risks during the period.	No exceptions noted.
		Inspected the risk assessment to determine that the risk assessment considered the Company's operational objectives, potential impacts and changes to the Company business model, and the potential for fraud and how fraud could have impacted the achievement of objectives.	No exceptions noted.
		Inspected the Insider Risk website to determine that the Company considered the potential for fraud and how fraud could have impacted the achievement of objectives within the risk assessment.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
	The Company has an established incident response policy that outlines management's responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the documented procedures for classification, prioritization, consolidation, and escalation of security incidents per criticality within the Information Security and Privacy Incident Response Policy to determine that the Company had established a documented incident response policy that outlined management's responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.
		Inspected security event tickets, post-mortem documentation, and customer communications for a sample of security events to determine that management implemented procedures to ensure quick, effective, and orderly responses to information security incidents.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company provides internal personnel with instructions and mechanisms for reporting potential security concerns or incidents to the responsible teams.	Inspected the Security Incident Response Policy and security incident reporting sites on the Company intranet to determine that the Company provided internal personnel with instructions and mechanisms for reporting potential security concerns or incidents to the responsible teams.	No exceptions noted.
	The Company has an established policy specifying that access to information resources, including data and the systems that store or process data, is required to be authorized based on the principle of least privilege.	Inspected the Identity and Access Management Policy to determine that access to information resources, including data and the systems that stored or processed data, was required to be authorized based on the principle of least privilege.	No exceptions noted.
	The Company establishes security policies and procedures that clearly define information security responsibilities for all employees. Within the information security policies and procedures, the Company assigns responsibilities to the Information Security team. The Company manages operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of products and services.	Inspected the Company's security policies and procedures to determine that the Company defined information security responsibilities for all employees, delegated decisions on risk identification and resource prioritization to various engineering groups, and assigned responsibilities to the Information Security team.	No exceptions noted.
		Inspected the risk assessment to determine that the Company managed operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly supported the operation of the Company's products and services.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Security policies are required to be reviewed and approved at least annually and created or updated as needed, and revised policies are required to be approved by authorized committees before they become valid. Security policies, supporting procedures, and guidelines are published on the intranet, which is accessible to all employees and contractors.	Inspected the Company's security policies on the intranet to determine that they were reviewed and approved at least annually and created or updated as needed and that revised policies were approved by authorized committees before they became valid.	No exceptions noted.
		Inspected the Security and Privacy Policy Creation and Maintenance process document to determine that security policies were required to be reviewed and approved annually and created or updated as needed and that revised policies were required to be approved by authorized committees before they became valid.	No exceptions noted.
		Inspected the security policies, procedures, and guidelines on the Company intranet to determine that security policies, supporting procedures, and guidelines were published on the Company intranet, which was accessible to all employees and contractors.	No exceptions noted.
	The Company develops and maintains a risk management framework to manage risk to an acceptable level. Company management evaluates risks by defining risk ratings and considers the risk of engaging with third parties.	Inspected the risk management guidelines to determine that the Company developed and maintained a risk management framework to manage risk to an acceptable level.	No exceptions noted.
		Inspected risk management guidelines and the risk assessment documentation to determine that Company management evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	No exceptions noted.
	The Company has established policies and guidelines to define customer data and govern data classification, labeling, and security.	Inspected the internal cloud compliance website, the DPST, and the Data Security Policy to determine that the Company established policies and guidelines to define customer data and govern data classification, labeling, and security.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company has implemented a vulnerability management program to detect and remediate system vulnerabilities. Remediation plans are developed, implemented, and tracked through remediation or to resolution for, at a minimum, all critical and high security deficiencies and are tracked within internal tools.	Inspected the Vulnerability Management Guidelines and the Vulnerability Priority Guidelines available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect and remediate system vulnerabilities and that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.
		Inspected tickets for a sample of security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools through remediation or to resolution for all critical and high security deficiencies identified during vulnerability detection activities.	No exceptions noted.
	The Company has developed policies, procedures, and tools that govern third-party relationships.	Inspected the Vendor Security Policy and support tool dashboards to determine that the Company had developed policies and procedures that governed third-party relationships.	No exceptions noted.
		Inspected third-party information and parameter requirements within the vendor directory tool used for controlling and monitoring third-parties to determine that the Company had developed policies, procedures, and tools that governed third-party relationships.	No exceptions noted.
	The Company has developed policies and procedures governing the secure development lifecycle.	Inspected the Security Design in Applications, Systems, and Services Policy and Source Code Guidelines to determine that the Company had developed policies and procedures governing the secure development lifecycle.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Change management policies, including security code reviews, are in place, and procedures for tracking, testing, approving, and validating changes are documented.	Inspected change management requirements and procedures within the Change Management Security Policy and documented source code guidelines to determine that change management policies, including security code reviews, were in place and that procedures for tracking, testing, approving, and validating changes were documented.	No exceptions noted.
	The Company has procedures in place to dispose of confidential information according to the data retention and deletion policy.	Inspected the Data Destruction Guidelines and User Data Retention and Deletion Guidelines to determine that the Company had procedures in place to dispose of confidential information according to the data retention and deletion policy.	No exceptions noted.
		Inspected the configuration of the automated deletion tool used to dispose of confidential information and data to determine that the Company implemented procedures to dispose of confidential information according to the data retention and deletion policy.	No exceptions noted.
	The Company maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers.	Inspected the Data Processing Terms on the publicly available Company website to determine that the Company maintained policies regarding the return, transfer, and disposal of user data and made these policies available to customers.	No exceptions noted.
	The Company has policies addressing security, confidentiality, and availability that have been approved by management and communicated to employees and are in accordance with ISO 27001.	Inspected the Company's security policies and procedures to determine that they addressed security, confidentiality, and availability and had been approved by management and were in accordance with ISO 27001.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the Company intranet accessible to all employees to determine that the Company had policies addressing security, confidentiality, and availability that had been communicated to employees.	No exceptions noted.
	The Company has established policies and procedures that govern the acceptable use of information assets.	Inspected the defined goals, roles, responsibilities, department coordination requirements, and the safeguards used for the compliance with legal and regulatory requirements defined in the Data Security Policy, the Data Classification Guidelines and procedures, and the Code of Conduct to determine that the Company had established policies and procedures that governed the acceptable use of information assets.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
	The Company has established guidelines for protecting against the risks of teleworking activities. Users can only access the system remotely through the use of encrypted communication systems.	Inspected the Company's Cryptographic Guidelines to determine that the Company had established guidelines for protecting against the risks of teleworking activities and that required the use of encrypted communication systems to access the system remotely.	No exceptions noted.
		Inspected the configuration that required the use of encryption to remotely authenticate to the system to determine that users could only access the system remotely through the use of encrypted communication systems.	No exceptions noted.
	Remote access to corporate machines requires a digital certificate issued by the Company installed on the connecting device, as well as two-factor authentication in the form of user ID, password, security key, and/or certificate.	Inspected the Company Certificate Authority Policy and the Account Authentication Security Policy to determine that remote access to corporate machines required a digital certificate issued by the Company installed on the connecting device and that it was required to enforce two-factor authentication in the form of user ID, password, security key, and/or certificate.	No exceptions noted.
		Inspected authentication configurations for remote access to corporate machines to determine that remote access to corporate machines required a digital certificate issued by the Company installed on the connecting device, as well as two-factor authentication in the form of user ID, password, security key, and/or certificate.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company has an established key management process in place to support the Company's use of cryptographic techniques.	Inspected the documented key management process within the Company's Cryptographic Guidelines to determine that the Company had an established key management process in place to support the Company's use of cryptographic techniques.	No exceptions noted.
		Inspected scan results showing enforcement of encryption and certificate authentication and revocation to determine that the Company had an established key management process in place to support the Company's use of cryptographic techniques.	No exceptions noted.
	Access to the corporate network, production machines, network devices, and support tools requires a unique ID, password, security key, and/or machine certificate.	Inspected authentication configurations for remote access to the corporate network, production machines, network devices, and support tools to determine that access to the corporate network, production machines, network devices, and support tools required a unique ID, password, security key, and/or machine certificate.	No exceptions noted.
	Only users with a valid user certificate, corresponding private key, and appropriate authorization (per host) can access production machines via Secure Shell (SSH).	Inspected the code that enforced the authentication of users prior to granting an authorized private key to determine that only users with a valid user certificate, corresponding private key, and appropriate authorization (per host) could access production machines via SSH.	No exceptions noted.
		Inspected the configuration enforcing authorized key authentication to determine that it restricted SSH access to production machines from unauthorized users without a valid digital certificate.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Access to network devices is authenticated via user ID, password, security key, and/or certificate.	Inspected the authentication configuration enforcing the required use of user IDs, passwords, security keys, and/or valid certificates for network device access to determine that access to network devices was authenticated via user ID, password, security key, and/or certificate.	No exceptions noted.
	Personnel access to sensitive internal systems and applications requires two-factor authentication in the form of a distinct user ID and password with a security key or certificate. Certificates are only generated after a user is authenticated to single sign-on using two-factor authentication.	Inspected the Account Authentication Guidelines to determine that personnel access to sensitive internal systems and applications was required to enforce two-factor authentication in the form of a distinct user ID and password with a security key or certificate.	No exceptions noted.
		Inspected the code that enforced the authentication of users prior to granting the user a certificate to determine that certificates that were required for access to sensitive internal systems and applications were only generated after a user was authenticated to single sign-on using two-factor authentication.	No exceptions noted.
	External system users are identified and authenticated via a multifactor authentication system before access is granted to cloud services.	Inspected the configuration providing external system users the ability to enforce multifactor authentication to determine that external system users were identified and authenticated via a multifactor authentication system before access was granted to cloud services.	No exceptions noted.
		Inspected the customer account creation process used by external system users to create their own password to determine that external system users were identified and authenticated via the multifactor authentication system before access was granted to cloud services.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company uses a version control system to manage source code, documentation, release labeling, and other functions.	Inspected the source code resources and Global Rollback procedures to determine that a version control system was required to be in place that was used to manage source code, documentation, and release labeling.	No exceptions noted.
		Inspected the version control system's rollback functionality and the code enforcing at least two levels of required approval by a separate technical resource prior to implementing changes to production to determine that the Company used a version control system to manage source code and other functions.	No exceptions noted.
	The Company has established formal guidelines for passwords to govern the management and use of authentication mechanisms. Authentication mechanisms are configured according to the guidelines.	Inspected the Guidelines for Google Passwords document to determine that the Company had established formal guidelines for passwords to govern the management and use of authentication mechanisms.	No exceptions noted.
		Inspected the SSH idle time configurations propagated to servers to determine that they were configured to enforce password requirements in accordance with established formal guidelines for authentication mechanisms.	No exceptions noted.
		Inspected corporate endpoint configurations to determine that users were locked out after a maximum of 15 minutes of inactivity in accordance with established formal guidelines for the management and use of authentication mechanisms.	No exceptions noted.
		Inspected the authentication configurations to determine that passwords were transmitted and stored in an encrypted procedure in accordance with established formal guidelines for passwords to govern the management and use of authentication mechanisms.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company segments networks based on the nature of services, users, and information systems being accessed.	Inspected the physical and logical network architecture and segmentation requirements for customer environments, infrastructure management, console management, and high risk environments within the Company's network diagrams and Network Access Security Policies to determine that the Company segmented networks based on the nature of services, users, and information systems that were being accessed.	No exceptions noted.
		Inspected the connection pathways of an example network within the network device monitoring tool and the configuration for access control and authentication requirements for production network access to determine that networks were segmented based on the nature of services, users, and information systems that were being accessed.	No exceptions noted.
	Customer data that is uploaded and created is required to be encrypted at rest. End users are able to control encryption keys.	Inspected the storage level encryption requirements for customer data within the Company's Cryptographic Guidelines to determine that customer data that was uploaded and created was required to be encrypted at rest.	No exceptions noted.
		Inspected the data backup encryption configurations and encryption configurations for storage devices with customer data to determine that customer data that was uploaded and created was encrypted at rest.	No exceptions noted.
		Inspected the Customer-Managed Encryption Keys guidance website to determine that encryption keys could be controlled by the end user.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company has an established policy specifying that access to information resources, including data and the systems that store or process data, is required to be authorized based on the principle of least privilege.	Inspected the Identity and Access Management Policy to determine that access to information resources, including data and the systems that stored or processed data, was required to be authorized based on the principle of least privilege.	No exceptions noted.
	Automated mechanisms are utilized to track inventory of production machines.	Inspected the Device Configuration Guidelines to determine that requirements for devices were documented and published to authorized users.	No exceptions noted.
		Inspected example asset exports and the configuration of the asset event monitoring tool that detected events and automatically updated the inventory management tool to determine that automated mechanisms were utilized to track and automatically update the inventory of production machines.	No exceptions noted.
	Access to internal support tools is restricted to authorized personnel through the use of approved credentials.	Inspected the configurations for TLS protocol and the enforcement of two-factor authentication in the form of user ID with password, security key, and/or certificate to determine that access to internal support tools was restricted to authorized personnel through the use of approved credentials.	No exceptions noted.
		Inspected the annual critical access group membership review evidence, a sample of critical access group members, and their respective job titles to determine that access to internal support tools was restricted to authorized personnel through the use of approved credentials.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Encryption is required to be used to protect user authentication and administrator sessions transmitted over the internet.	Inspected the Company's Cryptographic Guidelines regarding encryption mechanisms to determine that the Company required the use of encryption to protect user authentication and administrator sessions transmitted over the internet.	No exceptions noted.
		Inspected configurations around encryption mechanisms to determine that user authentication and administrator sessions transmitted over the internet were encrypted.	No exceptions noted.
		Inspected the server scan results to determine that the Company used encryption mechanisms to protect user authentication and administrator sessions transmitted over the internet.	No exceptions noted.
	Mechanisms are in place to detect attempts and prevent connections to the Company's network by unauthorized devices.	Inspected security group configurations to determine that mechanisms were in place to detect attempts and prevent connections to the Company's network by unauthorized devices.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
	Access to production machines, support tools, and network devices is managed via access control lists. Modifications to access control lists are recorded and approved by administrators.	Inspected access control lists and the configuration for group administrator approval requirements enforced by the access control system prior to provisioning user access to system components to determine that access to production machines, support tools, and network devices was managed via access control lists and that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the access control management tool and the documented approvals for a sample of transferred employees to determine that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.
	The Company separates duties of individuals by granting users access based on job responsibilities and least privilege and by limiting access to only authorized users.	Inspected the Account Security Policy and the Identity and Access Management Policy to determine that the Company separated duties of individuals by granting users access based on job responsibilities and least privilege and by limiting access to only authorized users.	No exceptions noted.
		Observed an attempt to access a privileged system outside the realm of the user's job responsibilities to determine that the attempt to violate the separation of duties failed and that the Company separated duties and implemented a principle of least privilege by limiting access to only authorized users.	No exceptions noted.
	Access to production machines, support tools, network devices, and corporate assets is automatically removed in a timely manner upon submission of a termination request by Human Resources or a manager.	Inspected the Identity and Access Management Policy to determine that the Company had documented procedures for terminating users with access to production machines, support tools, network devices, and corporate assets.	No exceptions noted.
		Inspected the configuration of the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets to determine that it was configured to automatically remove access in a timely manner upon submission of a termination request by Human Resources or a manager.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the historical account activity log and access removal evidence for an example terminated user's access to production machines, support tools, network devices, and corporate assets to determine that access was automatically removed in a timely manner by the automated tool used to revoke access upon submission of a termination request.	No exceptions noted.
	Critical access groups are reviewed at least annually to ensure that access is restricted appropriately, and reviews are tracked to completion.	Inspected the critical access groups' code configuration that assigned reviews to the authorized group administrators to determine that critical access groups were reviewed at least annually.	No exceptions noted.
		Inspected critical access group user membership reviews performed by group administrators to determine that critical access group memberships were reviewed at least annually to ensure that access was restricted appropriately and that reviews were tracked to completion.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.		
	Access to production machines, support tools, and network devices is managed via access control lists. Modifications to access control lists are recorded and approved by administrators.	Inspected access control lists and the configuration for group administrator approval requirements enforced by the access control system prior to provisioning user access to system components to determine that access to production machines, support tools, and network devices was managed via access control lists and that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the access control management tool and the documented approvals for a sample of transferred employees to determine that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.
	Access to production machines, support tools, network devices, and corporate assets is automatically removed in a timely manner upon submission of a termination request by Human Resources or a manager.	Inspected the Identity and Access Management Policy to determine that the Company had documented procedures for terminating users with access to production machines, support tools, network devices, and corporate assets.	No exceptions noted.
		Inspected the configuration of the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets to determine that it was configured to automatically remove access in a timely manner upon submission of a termination request by Human Resources or a manager.	No exceptions noted.
		Inspected the historical account activity log and access removal evidence for an example terminated user's access to production machines, support tools, network devices, and corporate assets to determine that access was automatically removed in a timely manner by the automated tool used to revoke access upon submission of a termination request.	No exceptions noted.
	Critical access groups are reviewed at least annually to ensure that access is restricted appropriately, and reviews are tracked to completion.	Inspected the critical access groups' code configuration that assigned reviews to the authorized group administrators to determine that critical access groups were reviewed at least annually.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected critical access group user membership reviews performed by group administrators to determine that critical access group memberships were reviewed at least annually to ensure that access was restricted appropriately and that reviews were tracked to completion.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
	The Company utilizes Google Cloud Platform (GCP) and Amazon Web Services (AWS) to host, maintain, and protect production servers, network devices, and network connections in data centers. GCP and AWS are carved out for the purposes of this report.	Not applicable.	Not applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
	The Company is required to sanitize storage media prior to disposal, release from Company control, or release for reuse.	Inspected the User Data Destruction and Retention Policy and guidelines to determine that the Company was required to sanitize storage media prior to disposal, release from Company control, or release for reuse.	No exceptions noted.
	The Company has procedures in place to dispose of confidential information according to the data retention and deletion policy.	Inspected the Data Destruction Guidelines and User Data Retention and Deletion Guidelines to determine that the Company had procedures in place to dispose of confidential information according to the data retention and deletion policy.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the configuration of the automated deletion tool used to dispose of confidential information and data to determine that the Company implemented procedures to dispose of confidential information according to the data retention and deletion policy.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
	Remote access to corporate machines requires a digital certificate issued by the Company installed on the connecting device, as well as two-factor authentication in the form of user ID, password, security key, and/or certificate.	Inspected the Company Certificate Authority Policy and the Account Authentication Security Policy to determine that remote access to corporate machines required a digital certificate issued by the Company installed on the connecting device and that it was required to enforce two-factor authentication in the form of user ID, password, security key, and/or certificate.	No exceptions noted.
		Inspected authentication configurations for remote access to corporate machines to determine that remote access to corporate machines required a digital certificate issued by the Company installed on the connecting device, as well as two-factor authentication in the form of user ID, password, security key, and/or certificate.	No exceptions noted.
	There are mechanisms in place to protect the production environment against a variety of denial of service (DoS) attacks.	Inspected the DoS Protection User Guide and incident management escalation playbooks to determine that mechanisms were in place to protect the production environment against a variety of DoS attacks.	No exceptions noted.
		Inspected the DoS thresholds, alerting configurations, and tickets created for example DoS alerts to determine that there were mechanisms in place to protect the production environment against a variety of DoS attacks.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company has implemented perimeter devices to protect the corporate network from external network attacks.	Inspected the policies, network topology diagrams, and firewall and global router configurations related to the perimeter devices to determine that the Company had implemented perimeter devices to protect the corporate network from external network attacks.	No exceptions noted.
	Encryption is required to be used to protect user authentication and administrator sessions transmitted over the internet.	Inspected the Company's Cryptographic Guidelines regarding encryption mechanisms to determine that the Company required the use of encryption to protect user authentication and administrator sessions transmitted over the internet.	No exceptions noted.
		Inspected configurations around encryption mechanisms to determine that user authentication and administrator sessions transmitted over the internet were encrypted.	No exceptions noted.
		Inspected the server scan results to determine that the Company used encryption mechanisms to protect user authentication and administrator sessions transmitted over the internet.	No exceptions noted.
	Mechanisms are in place to detect attempts and prevent connections to the Company's network by unauthorized devices.	Inspected security group configurations to determine that mechanisms were in place to detect attempts and prevent connections to the Company's network by unauthorized devices.	No exceptions noted.
	A host-based intrusion detection system (HIDS) is used to provide continuous monitoring of the Apigee API Management Platform environment and early detection of potential security breaches and is configured to send automated email alert notifications to security personnel when suspicious activity is detected.	Inspected HIDS configurations to determine that a HIDS was used to provide continuous monitoring of the Apigee API Management Platform environment and early detection of potential security breaches and was configured to send automated email alert notifications to security personnel when suspicious activity was detected.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
	The Company has established guidelines for protecting against the risks of teleworking activities. Users can only access the system remotely through the use of encrypted communication systems.	Inspected the Company's Cryptographic Guidelines to determine that the Company had established guidelines for protecting against the risks of teleworking activities and that required the use of encrypted communication systems to access the system remotely.	No exceptions noted.
		Inspected the configuration that required the use of encryption to remotely authenticate to the system to determine that users could only access the system remotely through the use of encrypted communication systems.	No exceptions noted.
	The Company maintains policies that define the requirements for the use of cryptography.	Inspected the Company's Cryptographic Guidelines and the Account Authentication Security Policy to determine that the Company maintained policies that defined the requirements for the use of cryptography.	No exceptions noted.
	The Company has established guidelines for governing the installation of software on organization-owned assets.	Inspected the Non-Google Software Installation Guidelines to determine that the Company had established guidelines for governing the installation of software on organization-owned assets.	No exceptions noted.
	The Company maintains policies for securing mobile devices used to access corporate network and systems.	Inspected the Mobile Device Security Guidelines to determine that the Company maintained policies for securing mobile devices used to access corporate network and systems.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company prohibits the use of removable media for the storage of Personally Identifiable Information (PII) and sensitive PII (SPII) unless the data has been encrypted.	Inspected the Removable Media Policy and the Company's Cryptographic Guidelines to determine that the Company prohibited the use of removable media for the storage of PII and SPII unless the data had been encrypted.	No exceptions noted.
	Encryption is required to be used to protect user authentication and administrator sessions transmitted over the internet.	Inspected the Company's Cryptographic Guidelines regarding encryption mechanisms to determine that the Company required the use of encryption to protect user authentication and administrator sessions transmitted over the internet.	No exceptions noted.
		Inspected configurations around encryption mechanisms to determine that user authentication and administrator sessions transmitted over the internet were encrypted.	No exceptions noted.
		Inspected the server scan results to determine that the Company used encryption mechanisms to protect user authentication and administrator sessions transmitted over the internet.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
	The Company has required the implementation of mechanisms to protect its information assets against malicious activity (e.g., malware, spam, phishing).	Inspected the Vulnerability Management Policy; Vulnerability Priority Guidelines; Security Design in Applications, Systems, and Services Policy; and the System Management Software Security Policy to determine that mechanisms such as antivirus, anti-malware, antispam, and anti-phishing tools were required to be in place to protect the Company's information assets against malicious activity.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the global policy configuration of antivirus, anti-malware, antispam, and anti-phishing tools installed on each in-scope operating system type to determine that mechanisms were implemented to protect the Company's information assets against malicious activity.	No exceptions noted.
	Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.	Inspected the Security and Privacy Incident Response Policy to determine that the Company documented the use of monitoring tools to send automated alerts to operational personnel based on predetermined criteria and that incidents were escalated per policy.	No exceptions noted.
		Inspected alert configurations and example alerts sent to operational personnel from monitoring tools to determine that monitoring tools were used to send automated alerts to operational personnel based on predetermined criteria and that incidents were escalated per policy.	No exceptions noted.
	The Company has implemented a vulnerability management program to detect and remediate system vulnerabilities. Remediation plans are developed, implemented, and tracked through remediation or to resolution for, at a minimum, all critical and high security deficiencies and are tracked within internal tools.	Inspected the Vulnerability Management Guidelines and the Vulnerability Priority Guidelines available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect and remediate system vulnerabilities and that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected tickets for a sample of security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools through remediation or to resolution for all critical and high security deficiencies identified during vulnerability detection activities.	No exceptions noted.
	The Company provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Inspected the Log Data Usage Rules, the Security Logging Policy, the Vulnerability Management Policy, and the System Management Software Security Policy on the Company intranet to determine that the Company provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	No exceptions noted.
		Inspected monitoring tool dashboards, alerting configurations, and example alerts to determine that the Company provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
	The Company has implemented a vulnerability management program to detect and remediate system vulnerabilities. Remediation plans are developed, implemented, and tracked through remediation or to resolution for, at a minimum, all critical and high security deficiencies and are tracked within internal tools.	Inspected the Vulnerability Management Guidelines and the Vulnerability Priority Guidelines available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect and remediate system vulnerabilities and that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.
		Inspected tickets for a sample of security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools through remediation or to resolution for all critical and high security deficiencies identified during vulnerability detection activities.	No exceptions noted.
	Procedures related to the management of information processing resources are made available by the Company. Procedures include guidance on requesting, monitoring, and maintaining resources and guidance around evaluating capacity demand.	Inspected the Company's resource management documentation to determine that procedures related to the management of information processing resources were made available by the Company and included guidance on requesting, monitoring, and maintaining resources and guidance around evaluating capacity demand.	No exceptions noted.
		Inspected the dashboard that monitored the use of resources and projected future capacity requirements to determine that the Company implemented procedures related to the management of information processing resources.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company conducts annual Information Security Risk Assessments to identify and evaluate risks, and the Company's operational objectives and potential impacts and changes to the Company business model are considered. This risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment performed for in-scope systems to determine that the Company conducted an Information Security Risk Assessment to identify and evaluate risks during the period.	No exceptions noted.
		Inspected the risk assessment to determine that the risk assessment considered the Company's operational objectives, potential impacts and changes to the Company business model, and the potential for fraud and how fraud could have impacted the achievement of objectives.	No exceptions noted.
		Inspected the Insider Risk website to determine that the Company considered the potential for fraud and how fraud could have impacted the achievement of objectives within the risk assessment.	No exceptions noted.
	The Company provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Inspected the Log Data Usage Rules, the Security Logging Policy, the Vulnerability Management Policy, and the System Management Software Security Policy on the Company intranet to determine that the Company provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	No exceptions noted.
		Inspected monitoring tool dashboards, alerting configurations, and example alerts to determine that the Company provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	No exceptions noted.
	System capacity is evaluated continuously, and system changes are implemented to help ensure that processing capacity can meet demand.	Inspected documentation of system capacity evaluations performed by management to determine that system capacity was evaluated continuously and system changes were implemented to help ensure that processing capacity could meet demand.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
	Audit logs are required to be continuously monitored for events related to security, confidentiality, and availability threats. Alerts are generated for further investigation.	Inspected the Information Security and Privacy Incident Response Policy to determine that audit logs were required to be continuously monitored for events related to security, availability, and confidentiality threats and that alerts were required to be generated for further investigation.	No exceptions noted.
		Inspected audit log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
		Inspected monitoring tool dashboards, alert threshold configurations, and examples alerts for events to determine that alerts were generated for further investigation.	No exceptions noted.
	Penetration tests are performed at least annually.	Inquired of management and inspected the annual penetration test to determine that penetration tests were performed at least annually.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all high and medium vulnerabilities identified during the annual penetration test.	Inspected remediation plans for vulnerabilities identified during the penetration test to determine that a remediation plan was developed and changes were implemented to remediate, at a minimum, all high and medium vulnerabilities identified during the annual penetration test.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company has geographically dispersed personnel from Security Incident Response Teams who are responsible for managing information security incidents and the investigations and dispositions of information security incidents.	Inspected internal incident response websites and the process in place for Security Incident Response Teams to quantify and monitor incidents within the Information Security and Privacy Incident Response Policy to determine that the Company had geographically dispersed personnel from Security Incident Response Teams who were responsible for the management of information security incidents and the investigations and dispositions of information security incidents.	No exceptions noted.
	Procedures related to the management of information processing resources are made available by the Company. Procedures include guidance on requesting, monitoring, and maintaining resources and guidance around evaluating capacity demand.	Inspected the Company's resource management documentation to determine that procedures related to the management of information processing resources were made available by the Company and included guidance on requesting, monitoring, and maintaining resources and guidance around evaluating capacity demand.	No exceptions noted.
		Inspected the dashboard that monitored the use of resources and projected future capacity requirements to determine that the Company implemented procedures related to the management of information processing resources.	No exceptions noted.
	The Company has implemented a vulnerability management program to detect and remediate system vulnerabilities. Remediation plans are developed, implemented, and tracked through remediation or to resolution for, at a minimum, all critical and high security deficiencies and are tracked within internal tools.	Inspected the Vulnerability Management Guidelines and the Vulnerability Priority Guidelines available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect and remediate system vulnerabilities and that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected tickets for a sample of security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools through remediation or to resolution for all critical and high security deficiencies identified during vulnerability detection activities.	No exceptions noted.
	There are mechanisms in place to protect the production environment against a variety of denial of service (DoS) attacks.	Inspected the DoS Protection User Guide and incident management escalation playbooks to determine that mechanisms were in place to protect the production environment against a variety of DoS attacks.	No exceptions noted.
		Inspected the DoS thresholds, alerting configurations, and tickets created for example DoS alerts to determine that there were mechanisms in place to protect the production environment against a variety of DoS attacks.	No exceptions noted.
	Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.	Inspected the Security and Privacy Incident Response Policy to determine that the Company documented the use of monitoring tools to send automated alerts to operational personnel based on predetermined criteria and that incidents were escalated per policy.	No exceptions noted.
		Inspected alert configurations and example alerts sent to operational personnel from monitoring tools to determine that monitoring tools were used to send automated alerts to operational personnel based on predetermined criteria and that incidents were escalated per policy.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Inspected the Log Data Usage Rules, the Security Logging Policy, the Vulnerability Management Policy, and the System Management Software Security Policy on the Company intranet to determine that the Company provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	No exceptions noted.
		Inspected monitoring tool dashboards, alerting configurations, and example alerts to determine that the Company provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	No exceptions noted.
	System capacity is evaluated continuously, and system changes are implemented to help ensure that processing capacity can meet demand.	Inspected documentation of system capacity evaluations performed by management to determine that system capacity was evaluated continuously and system changes were implemented to help ensure that processing capacity could meet demand.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
	The Company has an established incident response policy that outlines management's responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the documented procedures for classification, prioritization, consolidation, and escalation of security incidents per criticality within the Information Security and Privacy Incident Response Policy to determine that the Company had established a documented incident response policy that outlined management's responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected security event tickets, post-mortem documentation, and customer communications for a sample of security events to determine that management implemented procedures to ensure quick, effective, and orderly responses to information security incidents.	No exceptions noted.
	Security events are logged, tracked, resolved, and communicated to affected parties by management according to the Company's security incident response policies and procedures. All events are evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives.	Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives, and communicated to affected parties by management according to the Company's security incident response policies and procedures.	No exceptions noted.
	Penetration tests are performed at least annually.	Inquired of management and inspected the annual penetration test to determine that penetration tests were performed at least annually.	No exceptions noted.
	A remediation plan is developed and changes are implemented to remediate, at a minimum, all high and medium vulnerabilities identified during the annual penetration test.	Inspected remediation plans for vulnerabilities identified during the penetration test to determine that a remediation plan was developed and changes were implemented to remediate, at a minimum, all high and medium vulnerabilities identified during the annual penetration test.	No exceptions noted.
	The Company provides internal personnel with instructions and mechanisms for reporting potential security concerns or incidents to the responsible teams.	Inspected the Security Incident Response Policy and security incident reporting sites on the Company intranet to determine that the Company provided internal personnel with instructions and mechanisms for reporting potential security concerns or incidents to the responsible teams.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company maintains and communicates policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	Inspected the Information Security and Privacy Incident Response Policy and the procedures for reporting an incident on the Company intranet to determine that the Company maintained internal policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.
		Inspected the requirement for timely notifications of data breaches to affected customers, in accordance with disclosure laws or contractual agreements, within the Apigee Data Processing Addendum shared with customers to determine that the Company communicated policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.
	Audit logs are required to be continuously monitored for events related to security, confidentiality, and availability threats. Alerts are generated for further investigation.	Inspected the Information Security and Privacy Incident Response Policy to determine that audit logs were required to be continuously monitored for events related to security, availability, and confidentiality threats and that alerts were required to be generated for further investigation.	No exceptions noted.
		Inspected audit log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
		Inspected monitoring tool dashboards, alert threshold configurations, and examples alerts for events to determine that alerts were generated for further investigation.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
	The Company has an established incident response policy that outlines management's responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the documented procedures for classification, prioritization, consolidation, and escalation of security incidents per criticality within the Information Security and Privacy Incident Response Policy to determine that the Company had established a documented incident response policy that outlined management's responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.
		Inspected security event tickets, post-mortem documentation, and customer communications for a sample of security events to determine that management implemented procedures to ensure quick, effective, and orderly responses to information security incidents.	No exceptions noted.
	The Company provides internal personnel with instructions and mechanisms for reporting potential security concerns or incidents to the responsible teams.	Inspected the Security Incident Response Policy and security incident reporting sites on the Company intranet to determine that the Company provided internal personnel with instructions and mechanisms for reporting potential security concerns or incidents to the responsible teams.	No exceptions noted.
	The Company maintains and communicates policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	Inspected the Information Security and Privacy Incident Response Policy and the procedures for reporting an incident on the Company intranet to determine that the Company maintained internal policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the requirement for timely notifications of data breaches to affected customers, in accordance with disclosure laws or contractual agreements, within the Apigee Data Processing Addendum shared with customers to determine that the Company communicated policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	No exceptions noted.
	The Company has geographically dispersed personnel from Security Incident Response Teams who are responsible for managing information security incidents and the investigations and dispositions of information security incidents.	Inspected internal incident response websites and the process in place for Security Incident Response Teams to quantify and monitor incidents within the Information Security and Privacy Incident Response Policy to determine that the Company had geographically dispersed personnel from Security Incident Response Teams who were responsible for the management of information security incidents and the investigations and dispositions of information security incidents.	No exceptions noted.
	All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.	Inspected security event documentation to determine that all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the Company had recovered from the incidents.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
	The Company conducts disaster recovery (DR) and business continuity (BC) testing continuously (and requires it to be conducted at least annually) to enable infrastructure and application teams to test communication plans, failover scenarios, operational transitions, and other emergency responses. Participating teams create testing plans and document the results and lessons learned from the tests.	Inspected the DR and BC planning documentation, testing checklist, and testing results to determine that DR and BC testing was conducted by the infrastructure and application teams at least annually and that testing included communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.
		Inspected DR and BC testing documentation to determine that participating teams created testing plans and documented the results and lessons learned from the tests.	No exceptions noted.
	The Company has an established incident response policy that outlines management's responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the documented procedures for classification, prioritization, consolidation, and escalation of security incidents per criticality within the Information Security and Privacy Incident Response Policy to determine that the Company had established a documented incident response policy that outlined management's responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.
		Inspected security event tickets, post-mortem documentation, and customer communications for a sample of security events to determine that management implemented procedures to ensure quick, effective, and orderly responses to information security incidents.	No exceptions noted.
	All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.	Inspected security event documentation to determine that all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the Company had recovered from the incidents.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company has geographically dispersed personnel from Security Incident Response Teams who are responsible for managing information security incidents and the investigations and dispositions of information security incidents.	Inspected internal incident response websites and the process in place for Security Incident Response Teams to quantify and monitor incidents within the Information Security and Privacy Incident Response Policy to determine that the Company had geographically dispersed personnel from Security Incident Response Teams who were responsible for the management of information security incidents and the investigations and dispositions of information security incidents.	No exceptions noted.

Change Management			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
	System changes are documented, tested, reviewed, and approved by a separate technical resource before moving into production.	Inspected change request tickets for a sample of system changes to determine that system changes were documented, tested, reviewed, and approved by a separate technical resource before moving into production.	No exceptions noted.
	Changes to the Company's systems are tested before being deployed.	Inspected testing notes within change request tickets for a sample of system changes to determine that changes to the Company's systems were tested before being deployed.	No exceptions noted.
	Manual and automated changes to network configurations are reviewed and approved prior to deployment.	Inspected the documented change request tickets for a sample of manual network configuration changes to determine that manual changes to network configurations were reviewed and approved prior to deployment.	No exceptions noted.
		Inspected the documented change ticket for an example change released by the automated deployment tool based on a pre-configured network configuration change that was reviewed and approved through the manual change management process to determine that automated changes to network configurations were reviewed and approved prior to deployment.	No exceptions noted.
		Inspected tickets for a sample of changes made to the automated deployment tool to determine that automated changes to network configurations were reviewed and approved prior to deployment.	No exceptions noted.

Change Management			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company has developed policies and procedures governing the secure development lifecycle.	Inspected the Security Design in Applications, Systems, and Services Policy and Source Code Guidelines to determine that the Company had developed policies and procedures governing the secure development lifecycle.	No exceptions noted.
	The Company has established guidelines for governing the installation of software on organization-owned assets.	Inspected the Non-Google Software Installation Guidelines to determine that the Company had established guidelines for governing the installation of software on organization-owned assets.	No exceptions noted.
	A standard image is required to be utilized for the installation and maintenance of each production server.	Inspected the Change Management Policy and the Company Source Code Policy to determine that a standard image was required to be utilized for the installation and maintenance of each production server.	No exceptions noted.
		Inspected the approvals and configurations for baseline AMIs deployed to GCP and AWS servers to determine that a standard image was utilized for the installation and maintenance of each production server.	No exceptions noted.
	The Company uses a version control system to manage source code, documentation, release labeling, and other functions.	Inspected the source code resources and Global Rollback procedures to determine that a version control system was required to be in place that was used to manage source code, documentation, and release labeling.	No exceptions noted.
		Inspected the version control system's rollback functionality and the code enforcing at least two levels of required approval by a separate technical resource prior to implementing changes to production to determine that the Company used a version control system to manage source code and other functions.	No exceptions noted.

Change Management			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Development, testing, and build environments are separated from the production environment through the use of logical security controls.	Inspected the Security Design in Applications, Systems, and Services Policy and the Network Access Security Policy to determine that the Company separated the development, testing, and build environments from the production environment through the use of logical security controls.	No exceptions noted.
		Inspected access control groups and the separate development, testing, build, and production environments within example project workflow configurations to determine that the development, testing, and build environments were separated from the production environment through the use of logical security controls.	No exceptions noted.

Risk Mitigation			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
	The Company's information processing resources are distributed across distinct, geographically dispersed processing facilities, and backup restoration testing is completed and tracked via an audit log to support service redundancy and availability. The Company communicates customer responsibilities to support service redundancy and availability of their own data through the implementation of backups.	Inspected monitoring tool dashboard and the filesystem, datastore, and network configurations used for products and networks to determine that the Company's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
		Inspected Google's Data Processing Security Terms to determine that the Company communicated customer responsibilities to support service redundancy and availability of their own data through the implementation of backups for service and availability.	No exceptions noted.
		Inspected the replication tool dashboard and configurations to determine that the Company's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
		Inspected data and system restoration testing results for the in-scope databases restored during the period to determine that backup restoration testing was completed and tracked via an audit log to support service redundancy and availability.	No exceptions noted.

Risk Mitigation			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company develops and maintains a risk management framework to manage risk to an acceptable level. Company management evaluates risks by defining risk ratings and considers the risk of engaging with third parties.	Inspected the risk management guidelines to determine that the Company developed and maintained a risk management framework to manage risk to an acceptable level.	No exceptions noted.
		Inspected risk management guidelines and the risk assessment documentation to determine that Company management evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	No exceptions noted.
	The Company has an established incident response policy that outlines management's responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the documented procedures for classification, prioritization, consolidation, and escalation of security incidents per criticality within the Information Security and Privacy Incident Response Policy to determine that the Company had established a documented incident response policy that outlined management's responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.
		Inspected security event tickets, post-mortem documentation, and customer communications for a sample of security events to determine that management implemented procedures to ensure quick, effective, and orderly responses to information security incidents.	No exceptions noted.
	The Company provides internal personnel with instructions and mechanisms for reporting potential security concerns or incidents to the responsible teams.	Inspected the Security Incident Response Policy and security incident reporting sites on the Company intranet to determine that the Company provided internal personnel with instructions and mechanisms for reporting potential security concerns or incidents to the responsible teams.	No exceptions noted.

Risk Mitigation			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company conducts disaster recovery (DR) and business continuity (BC) testing continuously (and requires it to be conducted at least annually) to enable infrastructure and application teams to test communication plans, failover scenarios, operational transitions, and other emergency responses. Participating teams create testing plans and document the results and lessons learned from the tests.	Inspected the DR and BC planning documentation, testing checklist, and testing results to determine that DR and BC testing was conducted by the infrastructure and application teams at least annually and that testing included communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.
		Inspected DR and BC testing documentation to determine that participating teams created testing plans and documented the results and lessons learned from the tests.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		
	The Company takes a risk-based approach to reviewing the security practices of vendors and the security posture of vendor products. Reviews may include automated and manual assessments as determined by the sensitivity of data being processed or access being granted.	Inspected the Vendor Security Assessment Guidelines to determine that the Company had a documented, risk-based approach to reviewing the security practices of vendors and the security posture of vendor products.	No exceptions noted.
		Inspected the Vendor Security Audit review documentation for a sample of vendors to determine that the reviews included automated and manual assessments as determined by the sensitivity of data being processed or access being granted.	No exceptions noted.
	Cloud sub-processor security and privacy risks are assessed via semi-annual assessments of sub-processor control environments.	Inspected the Cloud Subprocessor Assessment Team Guidance documentation and the sub-processor control environment assessment documentation for a sample of cloud sub-processors to determine that semi-annual assessments of security and privacy risks of sub-processor control environments were performed.	No exceptions noted.

Risk Mitigation			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company has developed policies, procedures, and tools that govern third-party relationships.	Inspected the Vendor Security Policy and support tool dashboards to determine that the Company had developed policies and procedures that governed third-party relationships.	No exceptions noted.
		Inspected third-party information and parameter requirements within the vendor directory tool used for controlling and monitoring third-parties to determine that the Company had developed policies, procedures, and tools that governed third-party relationships.	No exceptions noted.
	The Company establishes agreements, including non-disclosure agreements (NDAs), for preserving confidentiality of information and software exchanges with external parties.	Inspected the NDA templates to determine that the Company's agreements, including NDAs, provided details on preserving confidentiality of information and software exchanges.	No exceptions noted.
		Inspected NDA acknowledgements for a sample of external parties to determine that the Company established agreements, including NDAs, for preserving confidentiality of information and software exchanges with external parties.	No exceptions noted.
	The Company has implemented an addendum to contract with processors (including sub-processors). The addendum defines the security obligations that the processor must meet to satisfy the Company's obligations regarding customer data.	Inspected the DPST template to determine that the DPST contained an addendum that defined the security obligations that processors (including sub-processors) had to meet to satisfy the Company's obligations regarding customer data.	No exceptions noted.
		Inspected the Inbound Service Agreement (ISA) and the Subprocessor Data Processing Agreement (SDPA) for a sample of processors and sub-processors supporting the in-scope systems to determine that the Company had implemented an addendum to contract with processors and sub-processors.	No exceptions noted.

Risk Mitigation			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the termination clause for service or product issues related to vendors within an example ISA to determine that it defined the security obligations that processors (including sub-processors) had to meet to satisfy the Company's obligations regarding customer data.	No exceptions noted.

Additional Criteria for Availability

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.		
	Procedures related to the management of information processing resources are made available by the Company. Procedures include guidance on requesting, monitoring, and maintaining resources and guidance around evaluating capacity demand.	Inspected the Company's resource management documentation to determine that procedures related to the management of information processing resources were made available by the Company and included guidance on requesting, monitoring, and maintaining resources and guidance around evaluating capacity demand.	No exceptions noted.
		Inspected the dashboard that monitored the use of resources and projected future capacity requirements to determine that the Company implemented procedures related to the management of information processing resources.	No exceptions noted.
	Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.	Inspected the Security and Privacy Incident Response Policy to determine that the Company documented the use of monitoring tools to send automated alerts to operational personnel based on predetermined criteria and that incidents were escalated per policy.	No exceptions noted.
		Inspected alert configurations and example alerts sent to operational personnel from monitoring tools to determine that monitoring tools were used to send automated alerts to operational personnel based on predetermined criteria and that incidents were escalated per policy.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Inspected the Log Data Usage Rules, the Security Logging Policy, the Vulnerability Management Policy, and the System Management Software Security Policy on the Company intranet to determine that the Company provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	No exceptions noted.
		Inspected monitoring tool dashboards, alerting configurations, and example alerts to determine that the Company provided monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	No exceptions noted.
	Production systems utilize cloud-hosted virtualized infrastructure to allow for increased capacity upon demand.	Inspected network diagrams and production systems to determine that cloud-hosted virtualized infrastructure was utilized to allow for increased capacity upon demand.	No exceptions noted.
	System capacity is evaluated continuously, and system changes are implemented to help ensure that processing capacity can meet demand.	Inspected documentation of system capacity evaluations performed by management to determine that system capacity was evaluated continuously and system changes were implemented to help ensure that processing capacity could meet demand.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.		
	The Company conducts disaster recovery (DR) and business continuity (BC) testing continuously (and requires it to be conducted at least annually) to enable infrastructure and application teams to test communication plans, failover scenarios, operational transitions, and other emergency responses. Participating teams create testing plans and document the results and lessons learned from the tests.	Inspected the DR and BC planning documentation, testing checklist, and testing results to determine that DR and BC testing was conducted by the infrastructure and application teams at least annually and that testing included communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected DR and BC testing documentation to determine that participating teams created testing plans and documented the results and lessons learned from the tests.	No exceptions noted.
	The Company's information processing resources are distributed across distinct, geographically dispersed processing facilities, and backup restoration testing is completed and tracked via an audit log to support service redundancy and availability. The Company communicates customer responsibilities to support service redundancy and availability of their own data through the implementation of backups.	Inspected monitoring tool dashboard and the filesystem, datastore, and network configurations used for products and networks to determine that the Company's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
		Inspected Google's Data Processing Security Terms to determine that the Company communicated customer responsibilities to support service redundancy and availability of their own data through the implementation of backups for service and availability.	No exceptions noted.
		Inspected the replication tool dashboard and configurations to determine that the Company's information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
		Inspected data and system restoration testing results for the in-scope databases restored during the period to determine that backup restoration testing was completed and tracked via an audit log to support service redundancy and availability.	No exceptions noted.
	Production systems utilize cloud-hosted virtualized infrastructure to allow for increased capacity upon demand.	Inspected network diagrams and production systems to determine that cloud-hosted virtualized infrastructure was utilized to allow for increased capacity upon demand.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Backups are required to be performed periodically to support the availability of customer data per contractual agreements.	Inspected the DPST and internal backup and restoration instructional guidelines to determine that backups were required to be performed periodically to support the availability of customer data per contractual agreements.	No exceptions noted.
		Inspected backup configurations and example backup logs to determine that backups were performed periodically to support the availability of customer data.	No exceptions noted.
	Formal procedures are documented that outline the process Google's staff follows to back up and recover customer data.	Inspected the backup and recovery procedures to determine that formal procedures were documented that outlined the process Google's staff followed to back up and recover customer data.	No exceptions noted.
	Restore tests are performed at least semi-annually to confirm the ability to recover customer data.	Inspected results of restoration of backup files for a sample of semi-annual restoration tests to determine that restore tests were performed at least semi-annually to confirm the ability to recover customer data.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
	The Company has implemented BC measures to maintain the availability of the Company's production infrastructure and services.	Inspected the Business Impact Analysis (BIA) documentation, the BC plan, and the Company's ISO 27001 Statement of Applicability to determine that requirements were established for BC measures that maintained the availability of the Company's production infrastructure and services.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the assigned roles, responsibilities, risks, and recovery objectives within the BC plan to determine that the Company had implemented BC measures to maintain the availability of the Company's production infrastructure and services.	No exceptions noted.
		Inspected documented recovery activities within the DR report to determine that recovery activities were outlined to maintain the availability of the Company's production infrastructure and services.	No exceptions noted.
	The Company conducts disaster recovery (DR) and business continuity (BC) testing continuously (and requires it to be conducted at least annually) to enable infrastructure and application teams to test communication plans, failover scenarios, operational transitions, and other emergency responses. Participating teams create testing plans and document the results and lessons learned from the tests.	Inspected the DR and BC planning documentation, testing checklist, and testing results to determine that DR and BC testing was conducted by the infrastructure and application teams at least annually and that testing included communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.
		Inspected DR and BC testing documentation to determine that participating teams created testing plans and documented the results and lessons learned from the tests.	No exceptions noted.
	Backups are required to be performed periodically to support the availability of customer data per contractual agreements.	Inspected the DPST and internal backup and restoration instructional guidelines to determine that backups were required to be performed periodically to support the availability of customer data per contractual agreements.	No exceptions noted.
		Inspected backup configurations and example backup logs to determine that backups were performed periodically to support the availability of customer data.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Formal procedures are documented that outline the process Google's staff follows to back up and recover customer data.	Inspected the backup and recovery procedures to determine that formal procedures were documented that outlined the process Google's staff followed to back up and recover customer data.	No exceptions noted.
	Restore tests are performed at least semi-annually to confirm the ability to recover customer data.	Inspected results of restoration of backup files for a sample of semi-annual restoration tests to determine that restore tests were performed at least semi-annually to confirm the ability to recover customer data.	No exceptions noted.

Additional Criteria for Confidentiality

Confidentiality			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
	The Company has established policies and guidelines to define customer data and govern data classification, labeling, and security.	Inspected the internal cloud compliance website, the DPST, and the Data Security Policy to determine that the Company established policies and guidelines to define customer data and govern data classification, labeling, and security.	No exceptions noted.
	Design documentation is required to be completed, reviewed, and approved before a feature launch is released that introduces new collection, processing, or sharing of user data.	Inspected the launch procedures and guidelines to determine that design documentation was required to be completed, reviewed, and approved before the release of a feature launch that introduced new collection, processing, or sharing of user data was released.	No exceptions noted.
		Inspected design documentation and launch tickets for example launches to determine that design documentation was completed, reviewed, and approved before the release of a feature launch that introduced new collection, processing, or sharing of user data was released.	No exceptions noted.
	Confidential or sensitive customer data is prohibited by policy from being used or stored in non-production systems or environments.	Inspected the Company User Data Access Policy and Guidelines for Accessing Corporate, Personal, and Test Accounts to determine that the use and storage of confidential or sensitive customer data in non-production systems or environments was prohibited by policy	No exceptions noted.
		Inspected the Company's test environments to determine that confidential or sensitive customer data was not used or stored in non-production systems or environments.	No exceptions noted.

Confidentiality			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The Company has procedures in place to dispose of confidential information according to the data retention and deletion policy.	Inspected the Data Destruction Guidelines and User Data Retention and Deletion Guidelines to determine that the Company had procedures in place to dispose of confidential information according to the data retention and deletion policy.	No exceptions noted.
		Inspected the configuration of the automated deletion tool used to dispose of confidential information and data to determine that the Company implemented procedures to dispose of confidential information according to the data retention and deletion policy.	No exceptions noted.
	The Company establishes agreements, including non-disclosure agreements (NDAs), for preserving confidentiality of information and software exchanges with external parties.	Inspected the NDA templates to determine that the Company's agreements, including NDAs, provided details on preserving confidentiality of information and software exchanges.	No exceptions noted.
		Inspected NDA acknowledgements for a sample of external parties to determine that the Company established agreements, including NDAs, for preserving confidentiality of information and software exchanges with external parties.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
	The Company has procedures in place to dispose of confidential information according to the data retention and deletion policy.	Inspected the Data Destruction Guidelines and User Data Retention and Deletion Guidelines to determine that the Company had procedures in place to dispose of confidential information according to the data retention and deletion policy.	No exceptions noted.

Confidentiality			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the configuration of the automated deletion tool used to dispose of confidential information and data to determine that the Company implemented procedures to dispose of confidential information according to the data retention and deletion policy.	No exceptions noted.
	The Company maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers.	Inspected the Data Processing Terms on the publicly available Company website to determine that the Company maintained policies regarding the return, transfer, and disposal of user data and made these policies available to customers.	No exceptions noted.
	The Company is required to sanitize storage media prior to disposal, release from Company control, or release for reuse.	Inspected the User Data Destruction and Retention Policy and guidelines to determine that the Company was required to sanitize storage media prior to disposal, release from Company control, or release for reuse.	No exceptions noted.