COALFIRE CONTROLS

Report on Google LLC's Description of Its Looker (Google Cloud core) Data Platform and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality Throughout the Period November 1, 2022 to March 31, 2023

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

Table of Contents

Section 1

Independent Service Auditor’s Report

COALFIRE CONTROLS

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 Looker (Google Cloud core) Data Platform Throughout the Period November 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 November 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 a subservice organization to provide infrastructure-as-a-service (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 organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

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 the Looker (Google Cloud core) Data Platform that was designed and implemented throughout the period November 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 November 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 organization 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 November 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 the Looker (Google Cloud core) Data Platform during some or all of the period November 1, 2022 to March 31, 2023, business partners of Google subject to risks arising from interactions with the Looker (Google Cloud core) Data 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
June 20, 2023

Section 2

Assertion of Google LLC Management

Google

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 Looker (Google Cloud core) Data Platform Throughout the Period November 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 Looker (Google Cloud core) Data 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 a subservice organization for infrastructure-as-a-service (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 organization.

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 the Looker (Google Cloud core) Data Platform that was designed and implemented throughout the period November 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 November 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 organization and user entities applied the complementary controls assumed in the design of Google's controls throughout that period.

Google

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

650 253-0000 main
Google.com

c. The controls stated in the description operated effectively throughout the period November 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 Looker (Google Cloud core) Data Platform Throughout the Period November 1, 2022 to March 31, 2023

Type of Services Provided

Google LLC (“Google”) provides Looker (Google Cloud core) Data Platform (“the Platform” or “Looker”), which is a software-as-a-service (SaaS) platform that delivers a business intelligence solution, embedded analytics application framework, and specific data applications. Its goal is to empower people through the smarter use of data. Looker (Google Cloud core) is a modern data platform, which aims to simplify the process of data visualization and distribution.

Platform Overview

The Platform provides a scalable, modern data analytics solution. Companies utilize their data teams to unify, transform, describe, and govern data from various data sources. This initial work by the data team allows business users across an organization to explore, visualize, and deliver data in Looker using an intuitive, web-based, point-and-click interface.

The Platform occupies the central part of customers’ data ecosystems, translating users’ business questions into Structured Query Language (SQL) queries, sending those queries to customers’ databases or data warehouses, and then presenting the results of those queries to users. Within Looker, customers manage database connections, users’ data access, and the data model that defines their business metrics in terms of raw data fields. Unlike many business intelligence tools, Looker does not store customers’ raw data. Instead, it only stores queries and query results in an encrypted format, and those results are either deleted or refreshed within 30 days.

The Platform does not write data to customers’ databases, with the exception of a “scratch schema” it uses for intermediate processing. It is recommended that customers restrict Looker’s database connection to read-only access outside of the scratch schema. Looker also provides an Action Hub that allows the customer to connect Looker to other services the customer is using (e.g., Salesforce, Google Ads, and GitHub) and write to those systems using their application programming interfaces (APIs). In addition to provisioning the Platform for use by their colleagues, the customer’s technical staff can also use Looker to build embedded analytic experiences for their own customers. Below is an overview of the Platform:

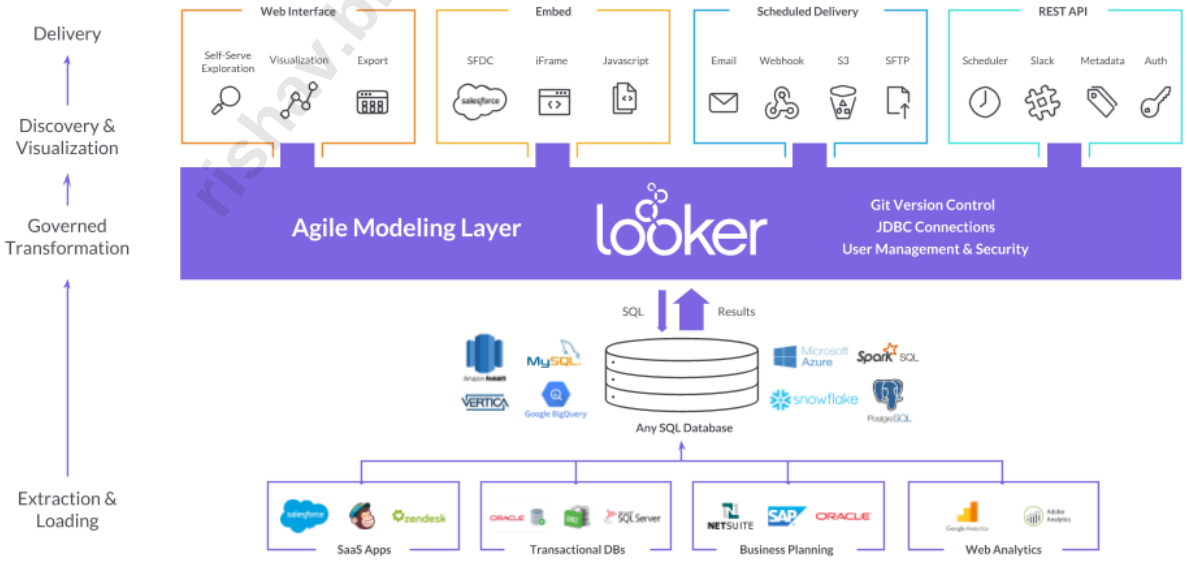

Figure 1: Looker Platform Overview

The primary features of the Looker (Google Cloud core) Hosted Data Platform are discussed in the following subsections.

Unification

As enterprises have become more data rich, the number of disparate sources (e.g., SaaS tools, Enterprise Resource Planning software, transactional databases, and advertising platforms) producing data has multiplied greatly. Accessing and linking that data presents both challenges and opportunities.

By connecting directly to multiple dialects of SQL, customers utilize the Platform to access their data in one tool. Using the Platform, customers can connect to transactional relationship database management systems (RDBMSs) (e.g., PostgreSQL and MySQL), traditional massively parallel processing (MPP) data appliances (e.g., Greenplum and Teradata), cloud MPP data warehouses (e.g., Amazon Redshift and Google BigQuery), SQL-on-Hadoop engines (e.g., Presto and Hive), and data virtualization engines (e.g., Denodo and DataVirtuality).

The Platform does not currently manage the extraction of data from source systems or the piping of data into relational databases, but it maintains partnerships with vendors who do. Once data is centralized in a warehouse or data lake, Looker unifies the view of that data.

Transformation

Whereas data transformation historically was performed before loading data into a warehouse, today's more powerful data engines allow more transformation to be executed at or near query time. Looker's proprietary data modeling language, LookML, provides a powerful, flexible, and reusable tool by which data analysts can share their knowledge about what data means to their business.

Governance

Google provides multiple ways to ensure individual employees are only able to access the data they are permitted to, including inheriting authentication roles from outside identity management systems, restricting access to analytic content or data down to the row and column level, and parameterizing connections to databases on a per-user basis.

LookML also provides strong governance, ensuring that the customer can define their business metrics, which are consistently applied when accessed by their non-technical users. LookML is version-controlled via Git, meaning that changes to the data model are logged, auditable, and capable of being rolled back to prior versions, if necessary.

Exploration and Visualization

The Platform's front-end interface allows non-technical users to view analytic content (dashboards and reports) created by others, to create their own analytic content, and to explore data in an ad-hoc fashion. Using Looker's front end does not require any technical knowledge, as operations are accomplished by pointing and clicking, and dashboard design is performed via dragging and dropping.

To further understand an ad hoc report, users with permissions are able to create rich, interactive visualizations of their data within Looker. These visualizations are fully customizable, and users can choose from a growing library of chart types to best represent their data.

Sharing, Delivery, and Action

The Platform is entirely browser-based, so that sharing analytic content with colleagues is as easy as sharing a link. As long as the recipient has proper permissions, they can view exactly what the sender was working on and collaborate with others.

Users with appropriate permissions are able to set up scheduled deliveries of data, dashboards, and reports via email, webhook, Amazon Simple Storage Service (Amazon S3) buckets, or Secure File Transfer Protocol (SFTP). Customers can use Looker's Action Hub to deliver data and content to additional destinations, as well as allowing users to take action on the analysis they view directly from within Looker (e.g., pausing an ad campaign on Google Ads or updating a Salesforce field from the Looker interface).

System Boundaries and Subservice Organizations

Included within the scope of this report are the Platform and the supporting production systems, infrastructure, software, people, procedures, and data. Any other Company services are not within the scope of this report.

The Platform utilizes third-party subservice organizations to provide the Platform, including Google Cloud for hosting the production environment and for the backup of Looker instance configurations.

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding Looker's performance. Commitments are documented and communicated in the Google Cloud Platform Terms of Service (Google Cloud ToS) (https://cloud.google.com/terms) (as of the date of this report). The Company's principal service commitments related to Looker, and relevant to security, availability, and confidentiality, are documented and communicated in the Google Cloud Data Processing Addendum (CDPA) (https://cloud.google.com/terms/data-processing-addendum) (as of the date of this report) and consists of the following:

- Looker will implement technical and organizational measures to protect customer data against accidental or unlawful destruction, loss, alteration, or access.
- Looker will implement and maintain technical and organizational measures to help ensure the ongoing availability, security, confidentiality, and resilience of Looker's systems and services.
- Looker will only use customer confidential information to exercise its rights and fulfill its obligations under the Terms of Service and will use reasonable care to protect against the disclosure of the customer confidential information.
- Looker 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 Looker 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 Looker 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
- Vulnerability scanning
- Encryption standards
- Subprocessor security
- Intrusion detection
- Incident response procedures
- Personnel security standards

The Components of the System Used to Provide the Services

The boundaries of the Platform 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 the Platform.

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

Infrastructure

Infrastructure consists of the data centers, Google Cloud cloud computing services, networks, systems, and other hardware powering the Platform. Infrastructure does not include any systems outside of the Looker production environment hosted on Google Cloud ("the Google Cloud production environment"), including its customers' database environment or third-party integrations.

Looker infrastructure is hosted in geographically distributed Google Cloud data centers, including those in the United States. During onboarding, customers can select where they would like their Looker instances to be physically hosted.

Google Cloud Cloud Computing Services

Google Cloud makes its infrastructure usable by abstracting it across specific cloud services. To operate the Platform, Looker uses the following Google Cloud services:

Infrastructure	
Service Name	**Description of Service**
Cloud Logging	Service that collects and monitors log files.
Google Computer Engine (GCE)	Cloud servers that host the Looker application, which includes systems that transmit, process, and temporarily store Customer Data. Such information may include personal information or other sensitive information depending on how customers choose to use Looker.

Infrastructure	
Service Name	**Description of Service**
Google Kubernetes Engine (GKE)	Cloud layer between GCE servers and containers running Looker app.
Google Container Registry	Service that provides storage for the container images used to run Looker application runtimes.
Google Filestore	Customer cluster deployments that provide storage across availability zones.
Cloud SQL	Service that provides SQL database storage.
Google Cloud Load Balancing	Service that performs network load balancing and distributed denial of service (DDoS) protections.
Google Cloud Build	Service that executes Looker images on Google infrastructure.
Google Cloud Identity and Access Management (IAM)	Service that provides control access to Google Cloud services and resources using IAM.
Google Cloud Pub/Sub	Service providing real-time messaging between independent services.
Google Managed Certificates – GKE	Domain name system (DNS) services.
Google Cloud Container Vulnerability Scanning Service	Service to scan containers that go into the registry.
Google Cloud BigQuery	Serverless data warehouse enabling scalable analytics.
Google Chime	Service used to send emails of scheduled reports.

Network Architecture

Looker users access the Platform through their browser over an encrypted connection. Looker front-end traffic passes through Global Load Balancer proxies before the request hits the customer's GKE runtimes.

Each customer has their own separate environment within the Google Cloud providing dedicated compute and storage. By default, a customer is set up with a cluster that can grow in size as demand increases. To further disperse load and provide additional redundancy, cluster configurations span multiple availability zones.

Internal Database Architecture

Each customer environment also has its own internal SQL database. A visual representation of the standard customer configuration is shown in the diagram below:

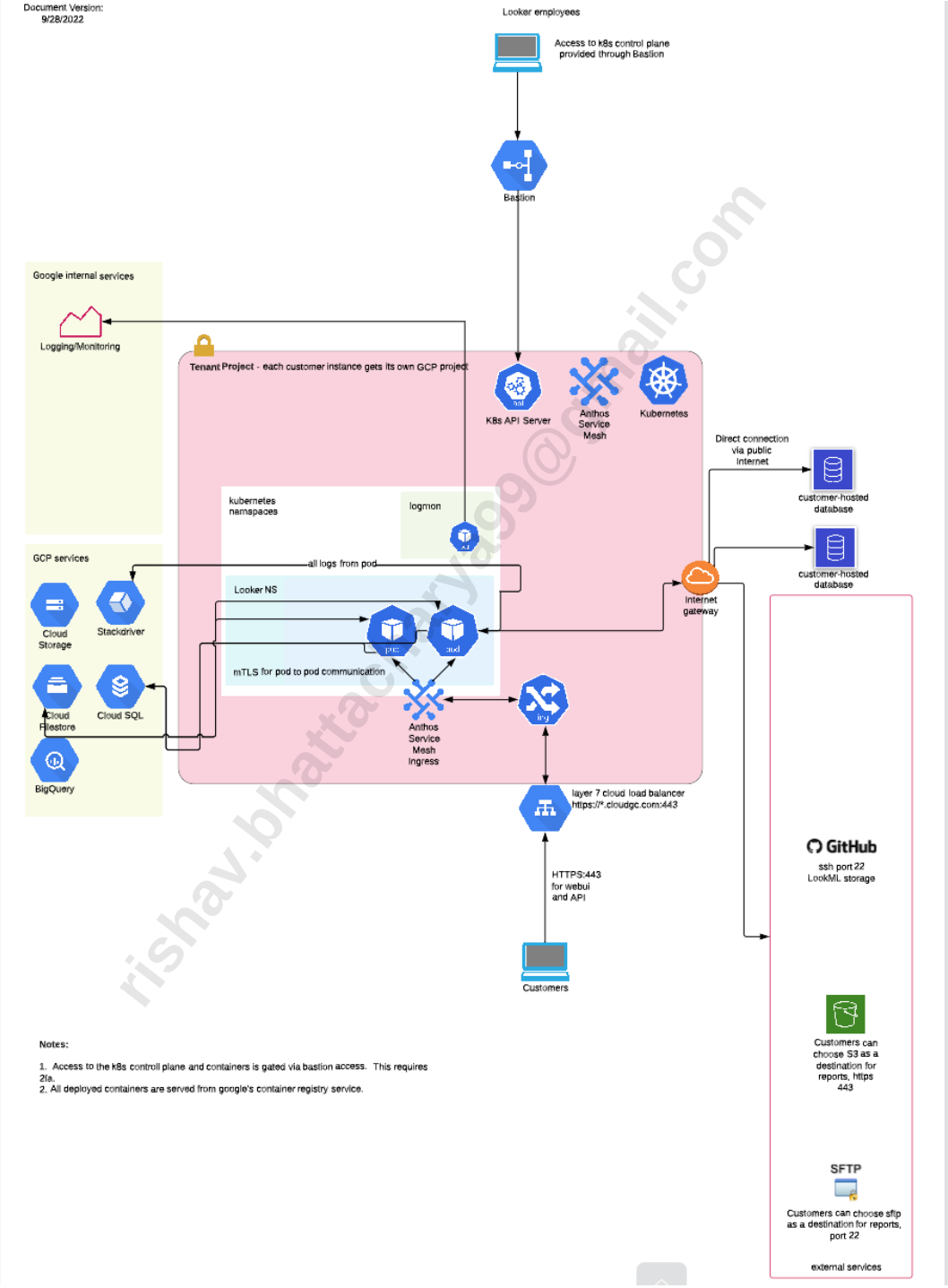

Figure 2: Looker (Google Cloud core) Data Platform Network Diagram

Software

Software consists of applications that support the Looker application. The Looker application is primarily written in JRuby, Java, Kotlin, Hypertext Markup Language 5 (HTML5), and JavaScript. Software is continuously developed, with major releases being deployed based on a release schedule.

Looker instances run the Linux operating system and utilize application packages such as MySQL to power the application. A new secure Linux image is built on a regular, continuous integration/continuous delivery (CI/CD) basis with the latest updates. This image is then placed into the hosted Looker deploy pipeline. In addition, hosts are continuously scanned for security vulnerabilities. Running containers are replaced to remediate identified vulnerabilities. Instances are also monitored for security-relevant deviations from the baseline. Any identified issues are triaged and documented.

Configuration management tools are used to set up each Looker instance to a secure baseline and to monitor any deviations from that baseline.

People

Google develops, manages, and secures the Platform via separate departments. The personnel primarily involved in the security governance, operation, and management of Looker includes the following:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
Human Resources (HR)	Responsible for user entity personnel recruiting and onboarding. This includes ensuring that controls related to employee backgrounds are defined.
Engineering, Product, and Design (EPD)	Responsible for designing, developing, testing, and deploying code to Looker's master branch in the code repository.
Production Engineering (ProdEng)	Responsible for maintaining the systems that Looker personnel use for developing and operating Looker's software. Additionally, this function is responsible for maintaining the Platform instances, networks used by those instances, and systems that grant authorized personnel access to the Google Cloud production environment. ProdEng also controls and builds production releases.
Customer Support	Responsible for providing technical support to customers' developers and administrators, primarily via online chat, but also via email and video conference. The Customer Support team is the primary point of contact for customer inquiries and issues with Looker's platform and helps them resolve issues with their instances. It is also responsible for passing information about ongoing customer problems and software bugs back to the EPD team.
Engineering Productivity (EngProd)/Release	Responsible for providing technical support to customers' developers and administrators, primarily via online chat, but also via email and video conference.
Customer Success	Responsible for tackling deeper technical and logistical issues with customers. Customer Success teams' partner to proactively identify and resolve customers' concerns and problems.

Data

Unlike most business intelligence tools, Looker does not ingest raw customer data. Instead, Looker leaves raw data in the customer datastore and writes derivations of that data, defined as Customer Data – including any information a customer or its end users create, input, submit, post, transmit, store, query, or display through the Looker service – back into the customer's proprietary datastore. In response to user questions, Looker writes SQL queries that retrieve the minimum amount of data necessary to answer the question and presents the results to the user. Internally, this data is stored in an encrypted cache and retained for no longer than 30 days. This approach minimizes the amount of Customer Data that Looker stores at any time.

Each Looker instance maintains its own local application database and disk storage, which contains the customer's data, including content from the instance; authentication credentials; metadata about the customer's data; usage logs; and encrypted, temporarily cached query results.

Looker also stores credential information, including those used to authenticate users to Looker (if native to Looker, no single sign-on [SSO] authentication is used) and those used by the platform to authenticate to the customer's datastores. Customer database credentials are encrypted using Advanced Encryption Standard (AES) encryption. Looker end user passwords are salted (mixed with random data) and hashed using bcrypt, a hashing utility. Clear-text user passwords are never written to the database. Instead, the application compares the results of the one-way hash with the password the end user enters to validate access.

The remainder of data that Looker stores is metadata, which covers application logging, histories of queries run, saved analytic content, and administration settings. Most of this data is stored in a local, internal database. The exception is application logs, which are stored as plain text files on a local disk.

The geographical locations of Looker instances are summarized in the table below:

Location	Google Cloud Region
US Central (Iowa)	us-central1
European Union (EU) (Netherlands)	europe-west4
Asia Pacific (APAC) (Sydney)	australia-southeast1

System 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 from November 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 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 Looker 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

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, which could include dismissal, lawsuits, and criminal prosecution.

The organization has utilized technologies to support the workforce in both remote and office work environment. As a result of the COVID-19 pandemic, functions requiring physical access to computer equipment and other hardware consider staff adjustments in order to maintain business operations and ensure safety of personnel.

System Requirements

Google has established internal policies and processes to support the delivery of Looker 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 Looker 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. Every employee has a written job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Google. Where local labor law or statutory regulations permit, Google may conduct criminal, credit, and/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 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 of and compliance with Google's Employee Handbook. The confidentiality and privacy of customer data is emphasized in the handbook and 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 Google. 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 Looker products provided by Google to user entities, irrespective of the location or business area. The Google teams which 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 Looker products. These risk management and mitigation activities are so critical that they have been integrated into Google's repeatable process model.

At a corporate level, there are multiple functional areas, including Legal, Information Security, Internal Audit, Privacy Engineering, Privacy Compliance, and Engineering Compliance, which provide risk management support through policy guidelines and internal consulting services.

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

Factors, including 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 exposed. The likelihood that a potential vulnerability could be exposed by a given threat-source is designated by Google as high, medium, or low.

Google then determines the potential adverse impact resulting from a 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 expose the vulnerability
- The effectiveness of existing security and privacy controls for mitigating 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, 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. Remediation of security and privacy deficiencies are tracked through internal tools and remediation plans.

Third-Party Risk Management

Google may utilize third-party vendors to support Looker. Prior to onboarding, Google completes the NDA and then performs the vendor security assessments (VSAs) on all vendors with whom Google shares confidential or sensitive information, including user data. A VSA is an important health check of a vendor's operational security posture. It assesses whether a vendor adheres to generally accepted security and data protection best practices. The outcome of a VSA is a risk assessment and an approval that determines if a vendor should or can be used. At a high level, each of these assessments involves:

- An initial risk assessment to determine whether a VSA is required (e.g., instances where vendors handle, collect, or access any user data, or business data that is classified as need-to-know)
- A risk-based review of the policies, processes, and controls the vendor has in place compared to generally accepted security best practices using questionnaire-based information gathering
- A tailored risk assessment for Mergers and Acquisitions due diligence or third-party risk management in partnerships, joint ventures, and other complex relationships
- Reviewing and citing independent verification of the security state of systems relevant to Google's use of the vendor

A subset of vendors are considered to be subprocessors based on the data sharing relationship between the vendor and Google. Google utilizes subprocessors to support Looker and has established expectations for subprocessors related primarily to security and privacy. The meeting of these expectations is subject to periodic review by Google. However, subprocessors do not manage or perform any Looker controls tested herein.

Google maintains a Subprocessor Audit Program that is tasked with the periodic information security and privacy assessment of subprocessors using ISO 27001 as the baseline. Google evaluates conformance to these expectations through inspection of third-party ISO certifications, SOC 2 reports, or on-site/virtual inspections. If Google identifies any deviations in the performance of subprocessor controls, findings are evaluated by Google and discussed with the subprocessors upon completion of the audit. When applicable, remediation plans are put in place to resolve issues in a timely manner.

Google has also implemented a Subprocessor Data Processing Agreement (SDPA) to contract with subprocessors. The SDPA defines the security and privacy obligations which the subprocessor must meet to satisfy Google's obligations regarding customer data, prior to Google granting such access. Per the Data Processing Addendum, Google notifies the customer prior to onboarding a new subprocessor. Information about the subprocessor, including function and location, is externally published (see https://cloud.google.com/terms/subprocessors).

Data Confidentiality and Privacy

Google has established training programs for privacy and information security to support data confidentiality. All Google personnel are required to complete these training programs within 90 days of joining the organization and annually thereafter. All new product and product-feature launches that include collection, processing, or sharing of user data are required to go through an internal security and privacy design review process. These reviews are performed by the security, legal, and privacy teams. Databases and websites exist to track and monitor progress of Looker project developments. In addition to the preventative controls, Google has also established detective measures to investigate and determine the validity of security threats. In the case of an incident, there are incident response processes to report and handle events related to topics such as security and confidentiality. Google establishes confidential agreements, including non-disclosure agreements, for preserving the confidentiality of information and software exchange with external parties.

Internal Functions and Policies

Formal organizational structures exist and are available to Google personnel on the Company's intranet. The intranet provides drill-down functionality for identifying personnel 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 and Privacy policies to establish procedures for information labeling and handling in accordance with the Google guidelines. Additionally, Google maintains policies that define the requirements for the use of cryptography and policies for securing mobile devices to help ensure company and customer data is protected. Policies are reviewed annually, and other materials derived from policies, like guidelines, FAQs, and other related documents, are reviewed and updated as needed.

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 and privacy training program that requires all employees to complete this training upon hiring
- Employees of the organization are required to acknowledge the Code of Conduct
- Regular management meetings for updates on business performance and other business matters
- Company goals and responsibilities are developed and communicated by management on a periodic basis and amended as needed. Results are evaluated and communicated to employees
- Detailed job descriptions; product information (including system and its boundaries); and Google's security, availability and confidentiality obligations that are made available to employees in the intranet

- The use of electronic mail messages to communicate time-sensitive messages and information
- Publishing security and privacy 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 Looker; and to help ensure that significant events are communicated to user entities in a timely manner. The primary conduit for communication is the Google web site, which is made available to all user entities. This includes blog postings on the Official Google Blog (https://blog.google/) (as of the date of this report) and various product specific blog support forums, and release notes. Google provides 24 x 7 assistance, including online and phone support to address customers' concerns. Customer service and/or 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 and/or developments, changes in services, and other information. Additionally, Google maintains an established Board of Directors that operates independently from management. The Board exercises oversight over management decisions.

As a data processor, Google limits processing to what is specified in the contracts with the controller or as otherwise required under applicable data protection laws. Customer data is processed in accordance with the Data Processing Addendum and is externally published (https://cloud.google.com/terms/data-processing-terms) (as of the date of this report). As data controllers, customers are responsible for communicating choices available to users regarding collection, use, retention, disclosure, and disposal of personal information. Google does provide customers with mechanisms to access, modify, delete, and export customer data.

Procedures

Procedures include the automated and manual procedures involved in operating Looker. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and HR. These procedures are drafted in line with overall information security policies.

The following subsections detail the procedures as they relate to the operation of the Platform.

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 and Privacy executive who is independent of Information Technology 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 that Google shares confidential or sensitive information with.

Google has security policies that 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.

Network Architecture and Management

The Looker system architecture utilizes a fully redundant network infrastructure. Border routers that provide the connection point between Looker and any Internet Service Providers are designed to run in a redundant configuration. Where border routers are in use, firewalls are also implemented to operate in a redundant configuration.

Google has implemented perimeter devices to protect the Google network from external attacks. Google segregates networks based on the types of services, users, and information systems. The network is managed via specialized tools. Google employs automated tools to inventory network devices and machines. Authorized security and network engineers access the network devices (production routers and switches) to monitor, maintain, manage, and secure the network through these tools.

Network monitoring mechanisms are in place to detect and disconnect access to the Google network from unauthorized devices. Configurations of perimeter devices are centrally managed. Current and previous versions of each router configuration are maintained. Google has documented procedures and checklists for configuring and installing new servers, routers, and switches on the network. The network is documented in network diagrams and configuration documents describing the nature of, and requirements applicable to, Google's production networks. This documentation resides within an access-restricted portion of the corporate intranet.

Google has a firewall configuration policy that defines acceptable ports that may be used on a Google firewall. Only authorized services and protocols that meet Google's requirements are permitted access to the network. The firewalls are designed to automatically deny all unauthorized packets not configured as acceptable. Administrative access to the firewalls is limited to authorized administrative personnel using the Secure Shell (SSH) protocol and two-factor authentication. Changes to network configurations are peer reviewed and approved prior to deployment. Google has implemented automated controls on network devices to identify DDoS attacks. Google has established incident response processes to report and handle such events (see the Incident Management section).

Mobile Device Management

Google has established policies to manage mobile device security. These policies list not only the approved devices, applications, and software, but also 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 Looker production systems, internal support tools, and customer data. Machine-level access restriction relies on Google-developed distributed authentication service based on Transport Layer Security (TLS) certificates which helps 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 Looker 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.

Google follows a formal process to grant or revoke employee access to Google resources. Lightweight Directory Access Protocol (LDAP), Kerberos, and a Google proprietary system that utilizes Secure Shell (SSH) and TLS certificates help provide secure and flexible access. These mechanisms are designed to grant access rights to systems and data only to authorized users.

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 are implemented to help ensure 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 on a semiannual basis 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 Looker 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 are 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 Looker 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 Looker are delivered as software releases. Change Management policies, including code reviews, are in place, and procedures for tracking, testing, approving, and validating changes are documented and implemented. Each service has documented release processes that specify the procedures to be used, including definition 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 a copy of the head source code files from the source code management system to modify them. Once development is complete, the developer initiates applicable testing and code reviews. Once the change has received the appropriate code review the changes can be submitted, making it the new head version. Google requires that a code reviewer be independent of the developer assigned and follows Google's coding standards.

Once the code is submitted, it can be used to build software binaries. During the build process, code is subject to automated testing, the results of which are monitored by engineers. Successfully built binaries can be migrated to staging or Quality Assurance (QA) environments where they can be subject to additional review. When software is ready for deployment to production, it is deployed in a controlled manner, with monitoring in place to notify engineers of anomalies in the deployment. The process from build to release is aided by several tools that automate tasks, including testing and deployment. Employees at Google have the ability to view changes, however, access to modify code and approve changes is controlled via functionality of internal tools that supports the build & release process.

Tools are also utilized to detect deviations from pre-defined Operating System (OS) configurations on production machines and correct them automatically. This allows for an easy roll out of updates to system files in a consistent manner and helps ensure that machines remain in a known current state.

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 at Google. 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 on an ongoing basis, to identify and remediate potential vulnerabilities.

Also, external third-party penetration tests are performed on an annual basis for a predetermined subset of the services included in Looker, and corrective actions are taken as necessary. The subset of services included in any given year are determined by the Google Security and Engineering Compliance teams and is 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 and incident response teams are responsible for managing, responding to, and tracking incidents. These teams are organized into formalized shifts and are responsible for helping resolve emergencies 24 x 7. Incident response policies are in place and procedures for handling incidents are documented.

Incident Alert and Recording

Log sources are used to generate alerts whenever an anomaly occurs. Production monitoring tools, in response to an anomaly, automatically generate alerts to relevant teams based on the anomaly

configurations set by each team. An anomaly may also be manually documented by a Google employee when an issue is identified or in response to a customer service request.

Production systems are configured to send system events to monitoring and alerting tools. Google personnel use these tools to respond to potential incidents, including security and privacy incidents.

Alerts capture information necessary for initial response (e.g., origin, service description, impacted area). Alerts are addressed by relevant teams to identify if the anomaly indicates an issue or potential issue. If necessary, incidents are created for alerts that require additional investigation. Additional details can be added to the incident to supplement the initial alert(s). The incident is assigned an initial severity level to prioritize mitigation efforts to incidents of greatest impact. Each severity level has been formally defined to capture the importance of each incident/problem type. There are established roles and responsibilities for personnel tasked with incident management, including the identification, assignment, managed remediation, and communication of incidents.

Incident Escalation

Google has documented escalation procedures and communication protocols that address the handling of incidents and notifying appropriate individuals. Escalated issues are treated with higher urgency and often shared with a wider audience.

Alert escalation is facilitated by an internal escalation tool or manual escalation based on Google-wide and team-specific escalation criteria. Production monitoring tools are integrated with the alert manager tool and communicate with the escalation tool via email and notification to on-call via pager. The escalation time and contacts are defined in the escalation tool configuration files. This leads to automated escalation if the tool does not receive an acknowledgement from the notified contacts.

Incident Resolution

After the necessary information about the incident is gathered, the incident ticket is assigned to the appropriate support area based on the nature of the problem and/or the root cause. Incidents are usually forwarded to one of the corresponding technical departments:

- System Reliability Engineers/Software Engineers
- Networks
- Database Administration
- System Administration
- Application Administration
- Facilities
- Network Security
- Platform Support
- Legal Team

The incident ticket is closed upon resolution of the incident. Google also has an established postmortem process for performing technical analysis of incidents after the fact to identify root cause issues, document lessons learned, and implement fixes to prevent future incidents. Processes for notifying customers of data security and privacy incidents that affect their accounts in accordance with disclosure laws or contractual agreements are established and implemented.

Data Retention and Deletion

Google has procedures in place to dispose of confidential and need-to-know information according to the Google data retention and deletion policy. Additionally, Google maintains defined terms regarding the return, transfer, and disposal of user data and makes these terms available to customers.

Backup and Recovery

A multi-region strategy for virtual machine scale sets is employed to permit the resumption of operations at other GCP regions in the event of the loss of a region. This provides high availability by dynamically load balancing across those sites. The Company 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 hardware failure, natural disaster, or other catastrophes, Google designs its infrastructure and services to be resilient to failures of software, hardware, or facilities. Redundant architecture and resources are distributed across at least two geographically dispersed data centers to support the availability of services. Network connections between the data centers help ensure swift failover. Management of the data centers is also distributed to provide location-independent, around-the-clock coverage and system administration.

Google's Disaster Recovery program enables continuous and automated 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, failover scenarios, operational transition, and other emergency responses. All teams that participate in the disaster recovery exercise develop testing plans and postmortems, which 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 process is accomplished through ongoing activities, separate evaluations, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that 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 maintaining and monitoring 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.
- Looker is monitored continuously using automated alerting tools.
- Management holds all-hands meetings as needed to communicate organizational results and objectives.

Separate Evaluations

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 confirm that the in-scope controls are consistently applied as designed, including whether manual controls are applied by individuals who have the competence and authority. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and 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, where personnel responsible for a particular unit or function will 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. In addition, departmental evaluations occur regularly as dictated by Company objectives. These evaluations document the assessment of the department evaluated and any process-level improvements that would help achieve the Company's company-wide goals. Any identified areas for improvement that could increase the effectiveness of the control environment are immediately discussed, analyzed, and implemented by the operations team where applicable.

Control Activities

Google's control activities are defined through its established policies and procedures. Policies are dictated through management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Logical and Physical Access

Management-approved business roles are used to determine Google Cloud production environment access for the different Looker business units. Employees are granted access to systems based on job function and associated business roles. Any exceptions require documented approval from a manager or above.

Access to sensitive systems and applications requires two-factor authentication in the form of a unique user ID, strong password, one-time password (OTP), security key, or certificates.

Periodic reviews of access lists are implemented to help ensure that access to customer data is appropriate and authorized. Access to production machines, network devices, and support tools is managed via an access group management system. The respective group administrators must approve membership in these groups. Critical user groups are reviewed bi-annually.

Access authorization in Looker 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 need to know, and it must be authorized and approved by the user's functional manager or system owners.

Production system access is granted only to individuals who have completed the required security training and require that level of access to perform their required tasks. Access to individual production systems is reviewed periodically by the system owners to ensure that access has been removed for employees who no longer have a business need for such access. The manager of any departing employee automatically removes access to all corporate and production resources upon submission of a termination request or by the appropriate HR manager.

Google Cloud Production Environment System Access ("The Back End")

Access to the customer's underlying operating system and database is managed using secure shell (SSH). Specifically, this access includes:

- *Google Cloud Management Console* – This provides the ability to manage the Google Cloud production environment, including adding and deleting customer instances, changing the Google Cloud security settings, and altering a number of other configurations. Administrative access to the Google Cloud management console is restricted to Operations personnel and requires two-factor authentication via username, password, and an authentication application.
- *Administration Access* – Leveraging Kubernetes and role-based authentication, specific users can gain shell access to the containers only in the event that an error cannot be solved via external tooling. Access to perform system administration is restricted to authorized users and controlled via multiple factors of authentication (username, password, and an authentication application).
- *Reduced Privileged Access* – Customer Support agents use external monitoring and administrative systems to view configurations, review logs, and troubleshoot customer containers.

Support Access ("The Front End")

Access to the customer's Looker application occurs via a web browser. The Support Access feature is limited to approved Looker employees based on job responsibilities and requires two-factor authentication via username, password, and authentication app. Customers can disable or grant specific time limits to the Support Access feature through a product configuration. The Support Access feature requires a logged business reason for each login and also requires the customer to enable the feature.

Ancillary Access

Access to tools that support the Looker application is restricted as follows:

- Configuration Management Tool – Looker uses a configuration management tool to centrally manage customer instances. Access to the configuration management tool is restricted to authorized personnel and requires bastion access to use.
- Code Repositories – Access to production source code is restricted to Engineering, Operations, Security, and Customer Support personnel (read-only access) and requires two-factor authentication.

Customer Access

Looker administrator and developer roles authenticate to the Looker application using a unique username and password or via SSO. Access to a customer's Looker application is associated with a unique web address. To protect against a brute force attack, the Looker application stores a password by first securely generating a high entropy (random) salt and then hashing the password and the generated value with modern password-hashing algorithms. The hashing part of the process is repeated thousands of times to prevent offline password attacks.

Production Network Controls

Looker uses Google Cloud to provide customer hosting. To ensure customer separation and protection from external threats, the Operations team maintains security groups and restricts inbound traffic to defined protocols and ports (e.g., 80 and 443).

To maintain the integrity and confidentiality of communications, Looker utilizes TLS to provide communication security over data transmissions between the Google Cloud production environment and external users.

Log File Protection and Privacy

Log files may contain sensitive information. To ensure log privacy and integrity, the platform maintains a centralized logging solution to protect this information from unauthorized disclosure and manipulation. Security event information is restricted from deletion or modification.

Corporate Endpoints

Endpoints are laptops and desktops used by Looker employees that may have access to interact with the Google Cloud production environment. Accordingly, these systems require the appropriate level of safeguards against potential threats. IT has responsibility for Looker endpoints and manages the configuration management software used to ensure that the security controls are enabled. These controls include:

- Encryption – Since they are portable and can be more easily lost or stolen, Looker laptops are encrypted and can be remotely wiped if misplaced.
- Antivirus – Endpoints run antivirus software with up-to-date virus definitions.
- Configuration – The endpoint management system notifies IT if there are attempts to modify or remove security software or controls.

Code Development

Google borrows concepts from DevOps and Agile methodologies in developing the Looker application. Looker releases occur every four weeks, with minor releases occurring between that window as needed. Organizationally, Engineering designs, codes, and tests the Looker application; Engineering Management approves the build for release; and Operations builds the release and deploys it to the Google Cloud production environment or makes the release available for download (on-premises). The Release Management Engineering team organizes the deployment steps and handles customer communications. This structure provides a segregation of responsibilities that enhance code quality and security.

Development and production environments are distinct and logically separated. Also, no Customer Data is used in development or testing. Only Operations personnel have the ability to deploy changes to the Google Cloud production environment. Developers have no write access to the Google Cloud management console or the Google Cloud production environment.

Code Testing

Automated code tests, including functional and regression testing, are performed on source code, and are required to pass prior to new code being merged to the master branch and deployed to production. Additionally, an engineer (who is not the code author) reviews and approves a code change before code is merged to the master branch. As an extra layer of testing, major releases have manual security, functionality, and usability tests performed prior to the release being deployed.

The Security team performs security architecture reviews of new features or significant changes in the Looker application architecture. In these scenarios, security architecture reviews are performed, and critical or high risks are remediated prior to code being deployed to the Google Cloud production environment.

Change Management

Infrastructure changes, including configuration changes, are maintained in a ticketing system. Depending on the nature of the change, these changes require peer review, management approval, or both, as dictated by policy, prior to deploying to production. New production servers are deployed using a standard image via a configuration management tool.

Data Retention and Disposal

Looker retains and disposes of Customer Data according to documented classification policies. By default, the Looker cache is refreshed at least every 30 days, ensuring that customer query results do not persist within the Looker environment past that time period. Looker management is required to approve customer data kept beyond the documented retention period or outside of stated purpose.

If a customer ends its subscription with Looker, this initiates an automated process that deletes the relevant Customer Data, including the customer's Looker configuration, usernames and passwords, database connection information, Google Cloud core instances, and internal databases within 30 days, as well as related backup information within one year.

Disaster Recovery and Business Continuity Management

Google knows that disasters can strike at any time and in any region or location. The infrastructure is designed for resilience and for restoration in case of service-impacting events. Looker provides disaster recovery and business continuity through multiple means. The Operations team monitors the Google Cloud

production environment continuously and is alerted when defined performance thresholds are surpassed. Backups are taken every 24 hours and stored outside the Google Cloud environment.

Performance Monitoring

Looker utilizes a wide variety of automated monitoring systems to provide a high level of security, service performance, and availability. Availability and capacity are also continuously monitored through a specific set of tools and control procedures. Event notifications are configured to notify management and Operations personnel when service thresholds are reached.

Automated tools monitor for potential issues that could affect system availability and performance. Notifications are sent to the Operations team and the on-call engineers when predefined thresholds are met. Significant issues are documented and tracked to resolution. Operations staff are on-call 24/7 to triage and resolve incidents related to security, availability, and confidentiality.

Backup Creation

Looker has defined a policy and procedures for performing backups that include coverage of backups, frequency of backups, management of backup media, and performance of restoration testing. By default, Looker application data is backed up every 24 hours, nightly, to Google Cloud Storage (GCS) for further redundancy. Backups are encrypted before being transmitted, and access to backups is restricted to administrators. Administrators can configure their Looker instances to use different backup settings or a different destination for backups.

Backup Restoration Testing

Looker conducts restoration tests quarterly. Results from these tests are recorded and reviewed regularly.

Availability

The availability category refers to the accessibility of the system or services as committed by Google's ToS. The platform's availability depends on many aspects of Google's operations, including cloud services and security functions. The risks that would prevent Google from meeting its availability commitments and requirements are diverse. Availability includes a consideration of risks during normal business operations and routine failure of elements of the system, and risks related to the continuity of business operations during a natural or man-made disaster.

Google has designed its controls to address the following availability risks:

- Insufficient processing capacity
- Insufficient Internet response time
- Loss of processing capability due to a power outage
- Loss of communication with user entities due to a break in telecommunication services
- Loss of key processing equipment, facilities, or personnel due to a natural disaster

Availability risks are addressed through the use and testing of various monitoring tools and backup and disaster recovery plans and procedures.

In evaluating the suitability of the design of availability controls, Google considers the likely causes of data loss, the commitments and requirements related to availability, the timeliness of backup procedures, the reliability of the backup process, and the ability to restore backed-up data. In evaluating the design of its

data availability controls, Google considers that most data loss does not result from disasters, but rather from routine processing errors and failures of system elements.

Confidentiality

Google has a data classification policy to classify data in one of three types, as described in the Data section above, based on how it is used or may be used in the service environment. There are three classifications for data:

- Need-to-Know
- Confidential
- Public

Retention periods and policies for ensuring retention during the specified period and proper disposal of data at the end of the retention period are also outlined in the data classification policy. The retention period assigned to data is based on (a) the classification of the data, (b) regulatory requirements and legal statutes, and (c) the general requirements of the business. During the designated retention period, Google ensures that backup media is stored in a protected environment for the duration of the designated document retention period. When the retention period has ended, Google destroys the information securely. Electronic information and other information are disposed of securely.

Complementary User Entity Controls (CUECs)

Google's controls related to the Platform cover only a portion of overall internal control for each user entity of the Platform. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by Google. Therefore, each user entity's internal control should be evaluated in conjunction with Google'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. • 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.

Criteria	Complementary User Entity Controls
CC6.4 CC6.5 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.

Subservice Organization and Complementary Subservice Organization Controls (CSOCs)

Google uses Google Cloud as a subservice organization for infrastructure-as-a-service (IaaS) services. Google's controls related to the Platform cover only a portion of the overall internal control for each user entity of the Platform. The description does not extend to the IaaS services for IT infrastructure provided by the subservice organization. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of Google and exclude the related controls of Google Cloud.

Although the subservice organization has 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 organization. CSOCs are expected to be in place at Google Cloud related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. Google Cloud's physical security controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Through its operational activities, Company management monitors the services performed by Google Cloud to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to Google Cloud management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to Looker 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 Google Cloud as described below.

Criteria	Complementary Subservice Organization Controls
CC6.4	• Google Cloud is responsible for restricting data center access to authorized personnel. • Google Cloud is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5 CC6.7	• Google Cloud is responsible for securely decommissioning and physically destroying production assets in its control.
CC7.2 A1.2	• Google Cloud is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • Google Cloud is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • Google Cloud is 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 Looker was used to provide the service from November 1, 2022 through March 31, 2023.

Report Use

The description does not omit or distort information relevant to Looker 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 November 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 the Looker (Google Cloud core) Data 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 organization has established a Code of Conduct that is reviewed and updated as needed.	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.
	Personnel of the organization are required to acknowledge the Code of Conduct.	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 organization has established 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 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 performed on new hires as permitted by local laws.	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 documentation 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 organization establishes confidentiality agreements with 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.
	The organization establishes confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information. The organization requires employees to sign these agreements upon employment.	Inspected employees' responsibilities and expected behavior for the protection of information within the confidentiality agreement template to determine that the Company established confidentiality agreements with employees to define responsibilities and expected behavior for the protection of information.	No exceptions noted.
		Inspected confidentiality agreement acknowledgements for a sample of employees to determine that employees acknowledged the Company's established confidentiality agreements that defined responsibilities and expected behavior for the protection of information upon employment.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
	All board of directors exercise independent judgment, while the independent / non-employee board of directors also demonstrate independence from management in exercising oversight of the development and performance of internal control.	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 that the board of directors met during the period.	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.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
	The organization 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.
	All board of directors exercise independent judgment, while the independent / non-employee board of directors also demonstrate independence from management in exercising oversight of the development and performance of internal control.	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 that the board of directors met during the period.	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.
	Company goals and responsibilities are required to be developed and communicated by management on a periodic basis, 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 security is managed by an executive who is dedicated to Security, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues.	Inspected the Security organizational charts on the Company's intranet to determine that information security was managed by an executive who was dedicated to Security, 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 executive met with relevant personnel to discuss security issues and was able to escalate security concerns to the board level as necessary.	No exceptions noted.
	New hires or 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**
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
	The organization 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.
	New hires or 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 performed on new hires as permitted by local laws.	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 documentation 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 organization has established a Code of Conduct that is reviewed and updated as needed.	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.
	Personnel of the organization are required to acknowledge the Code of Conduct.	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 organization has established 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 enforced a disciplinary process to address non-compliance with Company policies, the Code of Conduct, or other personnel requirements.	No exceptions noted.
	New hires or 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 is managed by an executive who is dedicated to Security, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues.	Inspected the Security organizational charts on the Company's intranet to determine that information security was managed by an executive who was dedicated to Security, 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 executive met with relevant personnel to discuss security issues and was able to escalate security concerns to the board level as necessary.	No exceptions noted.
	Company goals and responsibilities are required to be developed and communicated by management on a periodic basis, 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 organization reviews and validates the design, operation and control record of in-scope compliance controls on a periodic basis.	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 organization has an established Internal Audit function which evaluates management's compliance with security controls.	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 organization reviews and validates the design, operation and control record of in-scope compliance controls on a periodic basis.	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 organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect, remediate, and communicate system vulnerabilities and that remediation plans were required to be developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.
		Inspected detection activity results and example remediation tickets to determine that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and were tracked within internal tools.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The organization 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 continuously monitored for events related to security, availability, and confidentiality 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, confidentiality, and availability 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, confidentiality, and availability 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 organization 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 is managed by an executive who is dedicated to Security, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues.	Inspected the Security organizational charts on the Company's intranet to determine that information security was managed by an executive who was dedicated to Security, 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 executive met with relevant personnel to discuss security issues and was able to escalate security concerns 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 or 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 organization establishes security policies and procedures, which clearly define information security responsibilities for all employees. Within the information security policies and procedures, the organization assigns responsibilities to the Information Security team. The organization 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 / or 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 Google Looker system description within the Looker product site 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 organization'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.
	Inspected the Company intranet accessible to all employees to determine that the Company had policies addressing security, confidentiality, and availability that had been approved and made available to internal teams.	Inspected the Company's security policies and guidelines to determine that they addressed security, confidentiality, and availability; 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 approved and made available to internal teams.	No exceptions noted.
	Company goals and responsibilities are required to be developed and communicated by management on a periodic basis, 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 organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	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 organization's commitments to security, availability, and confidentiality are communicated to external users via publications such as the Terms of Service (ToS) and Cloud Data Processing Addendum (CDPA).	Inspected the Google Cloud Platform 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 Company's CDPA to determine that the Company's commitments to security, availability, and confidentiality were communicated to external users via publications.	No exceptions noted.
	The organization establishes agreements, including nondisclosure 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 organization requires external parties (Service Providers) to meet security & privacy requirements for safeguarding user data. Requirements are enforced via the "Information Protection Addendum (IPA)" or "Partner Information Protection Addendum (PIPA)" for service providers and partners, respectively.	Inspected the Cloud Data Processing Addendum (CDPA) template to determine that the CDPA 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 issues related to vendors within an example ISA and an example SDPA 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 Security Engineering Org 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 assessment 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.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		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.
	Changes to customer facing services that may affect security, confidentiality, and / or 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 organization 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 system documentation for Looker on the Company's external facing website that was available to existing customers 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.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Customer responsibilities are described on the organization's product websites or in system documentation.	Inspected customer responsibilities on Company 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 on the Company's product websites or in system documentation.	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 on a periodic basis, 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 organization develops and maintains a risk management framework to manage risk to an acceptable level.	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 organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	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.
	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 organization develops and maintains a risk management framework to manage risk to an acceptable level.	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 organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	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.
	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 organization has geographically dispersed personnel responsible for managing security incidents.	Inspected the security team internal webpage and the security team schedule to determine that the organization has geographically dispersed personnel responsible for managing security incidents.	No exceptions noted.
	The organization maintains a framework that defines how to organize a response to security & privacy 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 & privacy incidents.	No exceptions noted.
	The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected the Disaster Recovery (DR) and Business Continuity (BC) planning documentation and testing checklist to determine that DR and BC testing was required to be conducted at least annually and was required to include communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected Disaster Recovery (DR) and Business Continuity (BC) testing documentation and results for a sample of products to determine that the Company conducted DR and BC testing at least annually to enable infrastructure and application teams to test communication plans, failover scenarios, operational transitions, and other emergency responses, and 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 organization develops and maintains a risk management framework to manage risk to an acceptable level.	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 organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	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.
	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.	Inspected the annual penetration test results 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 organization develops and maintains a risk management framework to manage risk to an acceptable level.	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.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	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.
	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 organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect, remediate, and communicate system vulnerabilities and that remediation plans were required to be developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected detection activity results and example remediation tickets to determine that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and were tracked within internal tools.	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 organization has an established Internal Audit function which evaluates management's compliance with security controls.	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.	Inspected the annual penetration test results 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 Security Engineering Org 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 assessment 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.
	The organization reviews and validates the design, operation and control record of in-scope compliance controls on a periodic basis.	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**
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 organization has an established Internal Audit function which evaluates management's compliance with security controls.	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 Security Engineering Org 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 assessment 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.
	The organization reviews and validates the design, operation and control record of in-scope compliance controls on a periodic basis.	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 organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect, remediate, and communicate system vulnerabilities and that remediation plans were required to be developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.
		Inspected detection activity results and example remediation tickets to determine that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and were tracked within internal tools.	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 organization has an internal audit function and regularly engages independent parties to conduct reviews of the effectiveness of the organization's approach to managing information security and privacy. The results, including findings and corrective actions of these reviews are tracked and communicated to appropriate stakeholders.	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 was required to regularly engage with third parties to conduct independent reviews of the effectiveness of the Company's approach to managing information security and privacy.	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.
	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 organization develops and maintains a risk management framework to manage risk to an acceptable level.	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 organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	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 organization separates duties of individuals by granting users access based on job responsibilities and least privilege, and 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 organization develops and maintains a risk management framework to manage risk to an acceptable level.	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 organization has an internal audit function and regularly engages independent parties to conduct reviews of the effectiveness of the organization's approach to managing information security and privacy. The results, including findings and corrective actions of these reviews are tracked and communicated to appropriate stakeholders.	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 was required to regularly engage with third parties to conduct independent reviews of the effectiveness of the Company's approach to managing information security and privacy.	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.
	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 organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	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 organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	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 organization provides internal personnel (employees & extended workforce) with instructions and mechanisms for reporting potential security & privacy concerns or incidents to the responsible team(s).	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 and privacy concerns or incidents to the responsible teams.	No exceptions noted.
	The organization has an established policy specifying that access to information resources, including data and the systems which store or process data, is 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 organization establishes security policies and procedures, which clearly define information security responsibilities for all employees. Within the information security policies and procedures, the organization assigns responsibilities to the Information Security team. The organization 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.
	Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the Company's security policies and guidelines 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.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		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 organization develops and maintains a risk management framework to manage risk to an acceptable level.	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 organization has established policies and guidelines to govern data classification, labeling and security.	Inspected the internal cloud compliance website, the CDPA, and the Data Security Policy to determine that the Company had established policies and guidelines to define customer data and govern data classification, labeling, and security and that the Company's approach to meeting relevant statutory, regulatory, and contractual requirements was defined, documented, and updated at least annually.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect, remediate, and communicate system vulnerabilities and that remediation plans were required to be developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.
		Inspected detection activity results and example remediation tickets to determine that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and were tracked within internal tools.	No exceptions noted.
	The organization has policies and guidelines that govern third-party relationships.	Inspected the Vendor Security Policy and support tool dashboards to determine that the Company had developed policies and guidelines 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 tools that governed third-party relationships.	No exceptions noted.
	The organization has policies and guidelines 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 guidelines 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**
	The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	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 organization has procedures in place to dispose of confidential and need to know (ntk) 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 data deletion orders and data deletion tickets for a sample of customer requests for deletion to determine that the organization had procedures in place to dispose of confidential and need to know information according to the data retention and deletion policy.	No exceptions noted.
	The organization maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers.	Inspected the CDPA 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.
	Inspected the Company intranet accessible to all employees to determine that the Company had policies addressing security, confidentiality, and availability that had been approved and made available to internal teams.	Inspected the Company's security policies and guidelines to determine that they addressed security, confidentiality, and availability; 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 approved and made available to internal teams.	No exceptions noted.
	The organization has policies and guidelines 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 guidelines 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 organization 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 organization installed on the connecting device, and 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 organization has an established key management process in place to support the organization'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 the code configuration enforcing 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 corporate network, production machines, network devices, and support tools requires a unique ID, password, 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 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**
	Logical access to organization owned 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.	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 personnel access to sensitive internal systems and applications required two-factor authentication in the form of a distinct user ID and password with a security key or certificate and that certificates were only generated after a user was authenticated to single sign-on using two-factor authentication.	No exceptions noted.
	The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	Inspected the version control systems, rollback procedures, and change management tools to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions.	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, documentation, release labeling, and other functions.	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 organization has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	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 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.
	The organization segments production, corporate, and non-production networks based on their nature and usage. Networks are physically and/ or logically separated via access control mechanisms, only approved use cases are allowed, exceptions require additional review and approval.	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.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected example network connection pathways 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.
	The organization has an established policy specifying that access to information resources, including data and the systems which store or process data, is 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 organization maintains an up-to-date, accurate client device inventory.	Inspected the asset management tool and an example asset event log to determine that the organization maintained an up-to-date, accurate client device inventory and that automated mechanisms were utilized to track the inventory of production machines.	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 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.
	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 the CDPA website made available to external users regarding encryption mechanisms to determine that the Company communicated to external users on how user authentication and administrator sessions transmitted over the internet were encrypted.	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.
	Mechanisms are in place to detect attempts, and prevent connections to the organization's network by unauthorized devices.	Inspected Cloud Armor rule configurations, example alert configurations, and example alerts to determine that mechanisms were in place to detect attempts and prevent connections to the Company's network by unauthorized devices.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC6.2	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. Modification 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.
	The organization separates duties of individuals by granting users access based on job responsibilities and least privilege, and 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 basis 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 on a periodic basis and inappropriate access is removed.	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 for a sample of products 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. Modification 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**
	Access to production machines, support tools, network devices and corporate assets is automatically removed in a timely basis 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 on a periodic basis and inappropriate access is removed.	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 for a sample of products 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.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
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 GCP to host, maintain, and protect production servers, network devices, and network connections in data centers. GCP is 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 organization sanitizes storage media prior to disposal, release from organizational 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 organization has procedures in place to dispose of confidential and need to know (ntk) 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 data deletion orders and data deletion tickets for a sample of customer requests for deletion to determine that the organization had procedures in place to dispose of confidential and need to know 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**
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 organization installed on the connecting device, and 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.
	The organization has implemented mechanisms to protect the production environment from 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.
	The organization has implemented perimeter devices to protect the corporate network from external network attacks.	Inspected the policies, design documentation, 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.

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 the CDPA website made available to external users regarding encryption mechanisms to determine that the Company communicated to external users on how user authentication and administrator sessions transmitted over the internet were encrypted.	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.
	Mechanisms are in place to detect attempts, and prevent connections to the organization's network by unauthorized devices.	Inspected Cloud Armor rule configurations, example alert configurations, and example alerts to determine that mechanisms were in place to detect attempts and prevent connections to the Company's network by unauthorized devices.	No exceptions noted.
	Infrastructure supporting the service is updated through the use of customized and managed machine images and as a result of identified vulnerabilities in order to ensure that servers supporting the service are hardened against security threats.	Inspected a listing of approved Amazon Machine Images (AMIs) and example validated baseline configurations deployed to GCP servers to determine that infrastructure supporting the service was updated through the use of customized and managed machine images as a result of identified vulnerabilities in order to ensure that servers supporting the service were hardened against security threats.	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 organization 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 organization 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 organization 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 that governed the installation of software on organization-owned assets.	No exceptions noted.
	The organization maintains policies and guidelines for securing mobile devices used to access corporate networks and systems.	Inspected the Mobile Device Security Guidelines to determine that the Company maintained policies and guidelines for securing mobile devices used to access the corporate network and systems.	No exceptions noted.
	The organization prohibits the use of removable media for the storage of Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (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.

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 the CDPA website made available to external users regarding encryption mechanisms to determine that the Company communicated to external users on how user authentication and administrator sessions transmitted over the internet were encrypted.	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.
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 organization has implemented 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, antimalware, antispam, and antiphishing tools were required to be in place to protect the Company's information assets against malicious activity.	No exceptions noted.
		Inspected the global policy configuration of antivirus, antimalware, and antispam 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.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	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 required 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 organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect, remediate, and communicate system vulnerabilities and that remediation plans were required to be developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.
		Inspected detection activity results and example remediation tickets to determine that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and were tracked within internal tools.	No exceptions noted.
	The organization 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.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		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 organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect, remediate, and communicate system vulnerabilities and that remediation plans were required to be developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.
		Inspected detection activity results and example remediation tickets to determine that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and were tracked within internal tools.	No exceptions noted.
	The organization makes procedures related to the management of information processing resources available. 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 that procedures 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 organization conducts periodic Information Security Risk Assessments to identify and evaluate risks.	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 organization 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 continuously monitored for events related to security, availability, and confidentiality 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, confidentiality, and availability 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, confidentiality, and availability 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.	Inspected the annual penetration test results 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 organization maintains a framework that defines how to organize a response to security & privacy 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 & privacy incidents.	No exceptions noted.
	The organization has geographically dispersed personnel responsible for managing security incidents.	Inspected the security team internal webpage and the security team schedule to determine that the organization has geographically dispersed personnel responsible for managing security incidents.	No exceptions noted.
	The organization makes procedures related to the management of information processing resources available. 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 that procedures 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 organization has implemented a vulnerability management program to detect and remediate system vulnerabilities.	Inspected the Vulnerability Management Guidelines, the Vulnerability Priority Guidelines, and the online register of known vulnerabilities available on internal and external Company resources to determine that the Company had implemented a vulnerability management program to detect, remediate, and communicate system vulnerabilities and that remediation plans were required to be developed and implemented for, at a minimum, all critical and high security deficiencies and tracked within internal tools.	No exceptions noted.
		Inspected detection activity results and example remediation tickets to determine that remediation plans were developed and implemented for, at a minimum, all critical and high security deficiencies and were tracked within internal tools.	No exceptions noted.
	The organization has implemented mechanisms to protect the production environment from 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 required 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.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		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 organization 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**
CC7.3	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 organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	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.
	Security events are logged, tracked, resolved, and communicated to affected parties by management according to the organization'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.	Inspected the annual penetration test results to determine that penetration tests were performed at least annually.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	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 organization provides internal personnel (employees & extended workforce) with instructions and mechanisms for reporting potential security & privacy concerns or incidents to the responsible team(s).	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 and privacy concerns or incidents to the responsible teams.	No exceptions noted.
	The organization maintains policies and procedures regarding the notification of data breaches, 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 Looker 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.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Audit logs are continuously monitored for events related to security, availability, and confidentiality 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, confidentiality, and availability 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, confidentiality, and availability 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.
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 organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	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.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The organization provides internal personnel (employees & extended workforce) with instructions and mechanisms for reporting potential security & privacy concerns or incidents to the responsible team(s).	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 and privacy concerns or incidents to the responsible teams.	No exceptions noted.
	The organization maintains policies and procedures regarding the notification of data breaches, 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 Looker 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 organization has geographically dispersed personnel responsible for managing security incidents.	Inspected the security team internal webpage and the security team schedule to determine that the organization has geographically dispersed personnel responsible for managing security incidents.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The organization maintains a framework that defines how to organize a response to security & privacy 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 & privacy incidents.	No exceptions noted.
	All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the organization 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.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
	The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected the Disaster Recovery (DR) and Business Continuity (BC) planning documentation and testing checklist to determine that DR and BC testing was required to be conducted at least annually and was required to include communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.
		Inspected Disaster Recovery (DR) and Business Continuity (BC) testing documentation and results for a sample of products to determine that the Company conducted DR and BC testing at least annually to enable infrastructure and application teams to test communication plans, failover scenarios, operational transitions, and other emergency responses, and that participating teams created testing plans and documented the results and lessons learned from the tests.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	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 organization 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.
	The organization maintains a framework that defines how to organize a response to security & privacy 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 & privacy 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 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 organization'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.
	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 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 organization has policies and guidelines 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 guidelines governing the secure development lifecycle.	No exceptions noted.
	The organization 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 that governed the installation of software on organization-owned assets.	No exceptions noted.
	A standard image is 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 standard Looker image configurations and example production server images to determine that a standard image was required to be utilized for the installation and maintenance of each production server.	No exceptions noted.
	The organization uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved.	Inspected the version control systems, rollback procedures, and change management tools to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions.	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, documentation, release labeling, 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 development, testing, and build environments were separated 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 organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Inspected the 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 CDPA to determine that the Company communicated customer responsibilities to support service redundancy and availability of their own data through the implementation of backups within the Company's information processing resources.	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.
	The organization develops and maintains a risk management framework to manage risk to an acceptable level.	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.

Risk Mitigation			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		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 organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity.	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 organization provides internal personnel (employees & extended workforce) with instructions and mechanisms for reporting potential security & privacy concerns or incidents to the responsible team(s).	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 and privacy concerns or incidents to the responsible teams.	No exceptions noted.
	The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected the Disaster Recovery (DR) and Business Continuity (BC) planning documentation and testing checklist to determine that DR and BC testing was required to be conducted at least annually and was required to include communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.

Risk Mitigation			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected Disaster Recovery (DR) and Business Continuity (BC) testing documentation and results for a sample of products to determine that the Company conducted DR and BC testing at least annually to enable infrastructure and application teams to test communication plans, failover scenarios, operational transitions, and other emergency responses, and 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 Security Engineering Org 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 assessment 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 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 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 organization has policies and guidelines that govern third-party relationships.	Inspected the Vendor Security Policy and support tool dashboards to determine that the Company had developed policies and guidelines 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 tools that governed third-party relationships.	No exceptions noted.
	The organization establishes agreements, including nondisclosure 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 organization requires external parties (Service Providers) to meet security & privacy requirements for safeguarding user data. Requirements are enforced via the "Information Protection Addendum (IPA)" or "Partner Information Protection Addendum (PIPA)" for service providers and partners, respectively.	Inspected the Cloud Data Processing Addendum (CDPA) template to determine that the CDPA 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 issues related to vendors within an example ISA and an example SDPA 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.		
	The organization makes procedures related to the management of information processing resources available. 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 that procedures 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 required 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 organization 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 organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected the Disaster Recovery (DR) and Business Continuity (BC) planning documentation and testing checklist to determine that DR and BC testing was required to be conducted at least annually and was required to include 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 Disaster Recovery (DR) and Business Continuity (BC) testing documentation and results for a sample of products to determine that the Company conducted DR and BC testing at least annually to enable infrastructure and application teams to test communication plans, failover scenarios, operational transitions, and other emergency responses, and that participating teams created testing plans and documented the results and lessons learned from the tests.	No exceptions noted.
	The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.	Inspected the 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 CDPA to determine that the Company communicated customer responsibilities to support service redundancy and availability of their own data through the implementation of backups within the Company's information processing resources.	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.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		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.
	Backups are required to be performed periodically to support the availability of customer data per contractual agreements.	Inspected the 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 daily to support the availability of customer data.	No exceptions noted.
	Formal procedures are documented that outline the process which the Company'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 which the Company'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.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
	The organization has implemented business continuity measures to maintain the availability of its production infrastructure and services.	Inspected the BIA documentation, the Business Continuity (BC) Plan, and the Company's ISO 27001 Statement of Applicability to determine that requirements were established for business continuity measures that maintained the availability of the Company's production infrastructure and services.	No exceptions noted.
		Inspected the assigned roles, responsibilities, risks, and recovery objectives within the Business Continuity Plan to determine that the Company had implemented business continuity 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 organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected the Disaster Recovery (DR) and Business Continuity (BC) planning documentation and testing checklist to determine that DR and BC testing was required to be conducted at least annually and was required to include 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 Disaster Recovery (DR) and Business Continuity (BC) testing documentation and results for a sample of products to determine that the Company conducted DR and BC testing at least annually to enable infrastructure and application teams to test communication plans, failover scenarios, operational transitions, and other emergency responses, and 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 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 daily to support the availability of customer data.	No exceptions noted.
	Formal procedures are documented that outline the process which the Company'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 which the Company'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 organization has established policies and guidelines to govern data classification, labeling and security.	Inspected the internal cloud compliance website, the CDPA, and the Data Security Policy to determine that the Company had established policies and guidelines to define customer data and govern data classification, labeling, and security and that the Company's approach to meeting relevant statutory, regulatory, and contractual requirements was defined, documented, and updated at least annually.	No exceptions noted.
	Design documentation is required to be completed and be reviewed before a feature launch which 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.

Confidentiality			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the Company's test environments to determine that confidential or sensitive customer data was prohibited by policy from being used or stored in non-production systems or environments.	No exceptions noted.
	The organization has procedures in place to dispose of confidential and need to know (ntk) 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 data deletion orders and data deletion tickets for a sample of customer requests for deletion to determine that the organization had procedures in place to dispose of confidential and need to know information according to the data retention and deletion policy.	No exceptions noted.
	The organization establishes agreements, including nondisclosure 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.

Confidentiality			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
	The organization has procedures in place to dispose of confidential and need to know (ntk) 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 data deletion orders and data deletion tickets for a sample of customer requests for deletion to determine that the organization had procedures in place to dispose of confidential and need to know information according to the data retention and deletion policy.	No exceptions noted.
	The organization maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers.	Inspected the CDPA 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 organization sanitizes storage media prior to disposal, release from organizational 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.