COALFIRE CONTROLS

Report on Google LLC's Description of Its Google Distributed Cloud (GDC) connected and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality Throughout the Period November 1, 2023 to October 31, 2024

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

Google

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Google LLC ("Google")

Scope

We have examined Google's accompanying description in Section 3 titled "Google LLC's Description of Its Google Distributed Cloud (GDC) connected Throughout the Period November 1, 2023 to October 31, 2024" (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*), in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2023 to October 31, 2024, 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)*, in AICPA, *Trust Services Criteria*.

Google uses a subservice organization to provide cloud hosting 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 Google's GDC connected that was designed and implemented throughout the period November 1, 2023 to October 31, 2024, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period November 1, 2023 to October 31, 2024, 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 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, 2023 to October 31, 2024, 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 assumed in the design of Google's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Google, user entities of Google's GDC connected during some or all of the period November 1, 2023 to October 31, 2024, business partners of Google subject to risks arising from interactions with Google's GDC connected, 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 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
January 14, 2025

Section 2

Assertion of Google LLC Management

Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

650 253-0000 main
Google.com

Assertion of Google LLC ("Google") Management

We have prepared the accompanying description in Section 3 titled "Google LLC's Description of Its Google Distributed Cloud (GDC) connected Throughout the Period November 1, 2023 to October 31, 2024" (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*), in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about GDC connected 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)*, in AICPA, *Trust Services Criteria*.

Google uses a subservice organization for cloud hosting 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.

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

a. The description presents Google's GDC connected that was designed and implemented throughout the period November 1, 2023 to October 31, 2024, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period November 1, 2023 to October 31, 2024, 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 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, 2023 to October 31, 2024, 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 assumed in the design of Google's controls operated effectively throughout that period.

Google LLC

Section 3

Google LLC's Description of Its Google Distributed Cloud (GDC) connected Throughout the Period November 1, 2023 to October 31, 2024

Type of Services Provided

Google LLC (“Google” or “the Company”) is a global technology service provider focused on improving the ways people connect with information. Google maintains one of the world’s largest online indices of websites and other content, and it makes this information freely available to anyone with an Internet connection. Google’s automated search technology helps people obtain nearly instant access to relevant information from its vast online index.

Google Distributed Cloud (GDC) connected (also known as Google Distributed Cloud Edge [GDCE]) is a Google Cloud product that enables customers to run Google Kubernetes Engine (GKE) clusters on dedicated hardware provided and maintained by Google that is separate from the traditional Google Cloud data center. Google delivers and installs the GDC connected hardware on customer premises.

GDC connected enables customers to run 5G Core and radio access network (RAN) functions at the edge and also supports use cases for retail and enterprise applications such as:

- Anomaly detection using video and artificial intelligence (AI) to reduce defects on the factory floor.
- Real-time inventory with robots, enabling next-generation retail stores.
- Improving operational efficiency across automotive with sensors.
- Scrubbing sensitive data locally before it is transferred to the cloud.
- Hosting Point of Sale applications for retail environments.

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

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding GDC connected performance. The service organization’s security commitments in regard to the systems and operations are documented and communicated in Service Level Objectives (SLOs), Cloud Data Processing Addendums, Terms of Service, and other customer agreements and in the description of the service offering provided to user entities.

Those objectives are based on the service commitments that GDC connected makes to user entities; the laws and regulations that govern the provision of its services; and the financial, operational, and compliance requirements that GDC connected has established for the services.

Security commitments are standardized and include, but are not limited to, the following:

- Google will implement and maintain technical and organizational measures to protect customer data against accidental or unlawful destruction, loss, or alteration and unauthorized disclosure or access.
- Google will notify the customer promptly and without undue delay after becoming aware of a data incident and will promptly take reasonable steps to minimize harm and secure customer data.

- During the term of the agreement under which Google has agreed to provide the GDC connected system to the customer, the covered service will provide a monthly uptime percentage of at least 99.9%.
- Google will only access or use customer data to provide the services to the customer.
- Google will only use customer confidential information to fulfill its obligations and will use reasonable care to protect against the disclosure of customer confidential information.
- Google will disclose confidential information only to its affiliates, employees, agents, or professional advisors who have a need to know and who have agreed in writing to keep it confidential.
- Upon customer request, Google will return or delete customer data from Google's systems in accordance with applicable law.

System Requirements

System requirements are specifications regarding how GDC connected should function to meet the Company's 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 GDC connected include the following:

Google has established internal policies and processes to support the delivery of GDC connected 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 GDC connected 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 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.

The Components of the System Used to Provide the Services

The boundaries of GDC connected 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 GDC connected.

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

Infrastructure

The Company utilizes Google Cloud Platform (GCP) and Google corporate resources to provide the resources to support GDC connected. The Company leverages these experiences and resources to scale quickly and securely as necessary to meet current and future demand. The Company leverages multiple regions and multiple availability zones to provide redundancy and increase the availability of the services.

Google provides, deploys, operates, and maintains a rack of dedicated hardware that runs the customer GDC connected zone. This hardware consists of rack-mounted server machines and two top-of-rack (ToR) switches that connect the machines with the customer local network. The GDC connected nodes that execute customer workloads run exclusively on this hardware.

GDC connected nodes are not standalone resources and must remain connected to GCP for control plane management and monitoring purposes. The GDC connected control plane nodes are hosted in the designated GCP region. The GCP region for the customer GDC connected zone is determined by the location of the Google data center that is the closest to the GDC connected installation.

Infrastructure			
Production Tool	**Business Function**	**Operating System**	**Hosted Location**
One Platform application programming interfaces (APIs), GKE Hub	Managed control plane	Google Cloud Stack	GCP
Shax, Asset service, Stoat	Fleet management	Google Prod Stack	Google datacenters
Edge Network	Network configuration	Google Prod Stack	Google datacenters
Anthos	Cluster management	Kubernetes	Customer datacenter

The following workflow diagram reflects the GDC connected internal structure related to the tools discussed above:

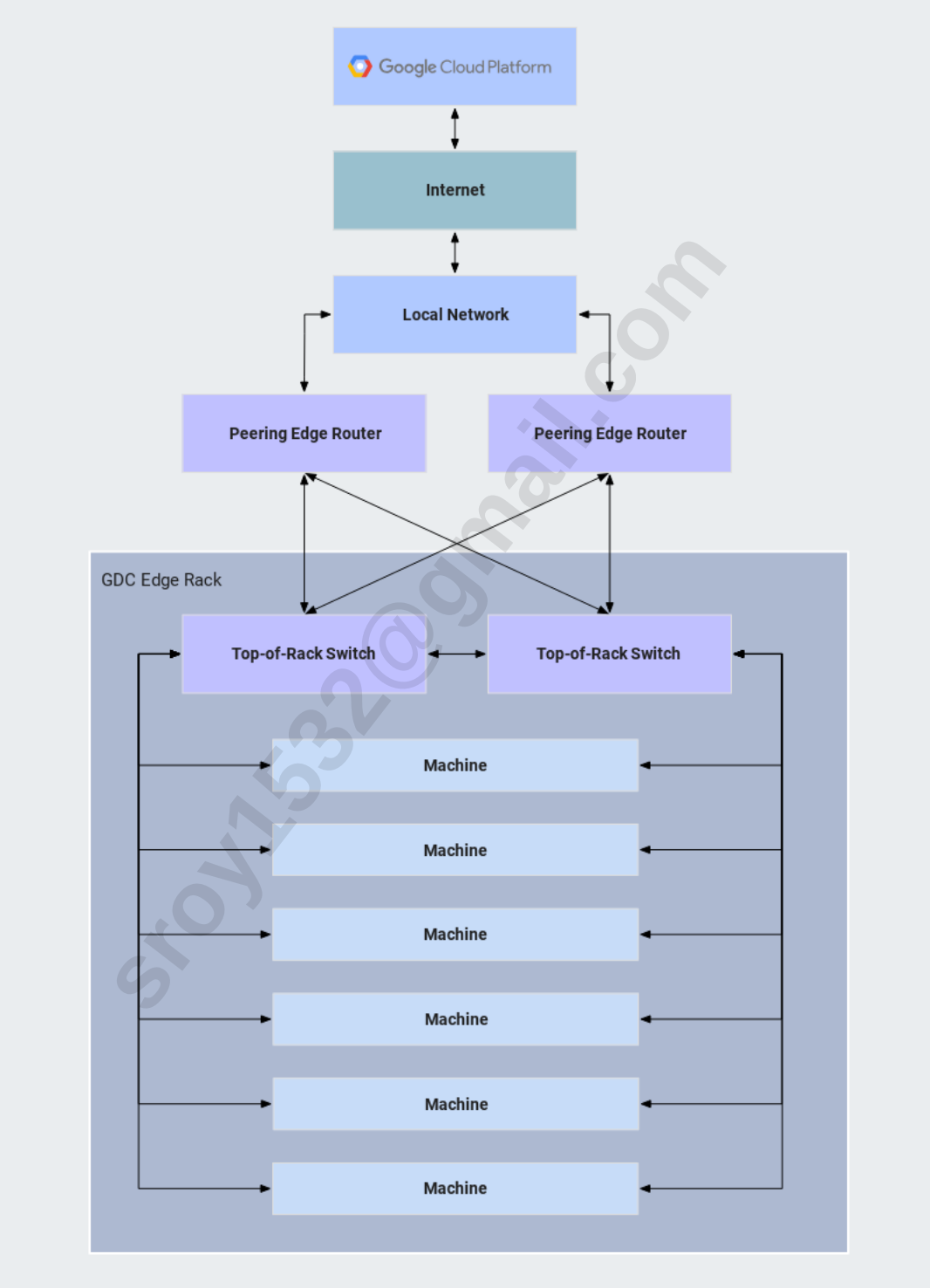

Figure 1: GDC connected Components

Software

Software consists of the programs and software that support GDC connected (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor GDC connected includes the following applications, as shown in the list below:

- Deployed (on-premises)
  - EdgeOS - A "board" (variation) of ContainerOS
  - GDC-E Network Automation (GNAS)- The server component encompasses all logic that handles network fabric APIs as well as the internal APIs
  - Metrics Forwarder
  - Machine Agent - A system daemon running in the OS. It is responsible for managing machine resources such as bootstrapping and upgrading the Kubernetes cluster and managing the machine identity
  - Anthos - A distribution of Kubernetes sourced from GKE
  - Ceph and Robin.io software defined storage for K8s
  - Cilium Container Network Interface (CNI), Istio, Envoy - Network management
  - Anthos Network Gateway (ANG), Anthos network controller, metallb (load balancer for bare metal Kubernetes clusters)
- Backend (in Prod)
  - QBONE (global) - QUIC-based virtual private network (VPN) for connecting edge machines with Google Prod
  - Riker (global) - Fleet management actuator
  - Software as a service (SaaS) management (regional) - Managing cluster control plane, including health checks and monitoring
  - Google Compute Engine (GCE) (regional/zonal) - Running control plane virtual machines (VMs) and load balancers
  - Net Model Actions (NMA) (global) - Configures network topology
  - Shax, Rackinfo (global) - Source of truth for machine assets
  - Spanner (regional) - Storing and querying network model
  - Stoat (global) - Configures network topology
  - Edge API server
- GCP
  - Cloud Key Management Service (Cloud KMS) (regional) - Per-cluster key management
  - GKE Connect/Hub (global) - Managing cluster memberships
  - Identity and Access Management (IAM) (regional) - Resource authorization
  - Google Compute Engine
  - Google Cloud Storage

People

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

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Operations Management	Responsible for day-to-day management of the services, including defining platform availability and security and providing customer support.
Software Development	Responsible for new version releases and support for internally escalated issues from operations departments.
Human Resources (HR)	Responsible for user entity personnel recruiting and onboarding. This includes ensuring that controls related to employee backgrounds are defined.

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, 2023 to October 31, 2024.

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.

Relevant Aspects of Internal Control

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

- Control Environment – Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- Risk Management – The entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks should be managed across the internal and external control environment, including third-party risk.

- Information and Communication – Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange information needed to conduct and control its operations.
- Monitoring – The entire process must be monitored, with modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.
- Control Activities – Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to the achievement of the entity's control objectives are effectively carried out.

This section briefly describes the essential characteristics and other interrelated components of internal controls and divides them into four broad areas. These areas support the achievement of the applicable Trust Services Criteria for security, availability, and confidentiality as they pertain to the GDC connected 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 noncompliance with the code of conduct, security policy, and other personnel requirements, which could include dismissal, lawsuits, and criminal prosecution.

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.

Risk Management

Risk management is a pervasive component of the GDC connected products provided by Google to user entities, irrespective of the location or business area. The Google teams that lead engineering, sales, customer service, finance, and operations have the primary responsibility to understand and manage the risks associated with their activities for user entities using GDC connected 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, that 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 GDC connected. 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, the nature of the vulnerability, and the 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 GDC connected. Prior to onboarding, Google completes the nondisclosure agreement (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

Subprocessors are a subset of vendors based on the data sharing relationship between the vendor and Google. Google utilizes subprocessors to support GDC connected 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 GDC connected 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. 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 that 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 annually. 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 GDC connected 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 NDAs, 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, such as guidelines, frequently asked questions (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 annually
- Requiring employees of the organization to acknowledge the code of conduct
- Regular management meetings for updates on business performance and other business matters
- Company goals and responsibilities, which are developed and communicated by management periodically and amended as needed, the results of which 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 on the intranet
- The use of email 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 GDC connected and to help ensure that significant events are communicated to user entities in a timely manner. The primary conduit for communication is the Google website, which is made available to all user entities. This includes blog postings on the Official Google Blog (https://blog.google/) (as of the date of this report) and various product-specific blog support forums and release notes. Google provides 24/7 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 provides customers with mechanisms to access, modify, delete, and export customer data.

Procedures

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.

Procedures include the automated and manual procedures involved in operating GDC connected. 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 GDC connected.

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 IT management responsibilities and may escalate security issues or concerns directly to the board. The security team also reviews the security practices of vendors and the security posture of vendor products for all vendors with whom Google shares confidential or sensitive information.

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

Network Architecture and Management

The GDC connected system architecture utilizes a fully redundant network infrastructure. Border routers that provide the connection point between GDC connected 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 distributed denial-of-service (DDoS) attacks. Google has incident response processes to report and handle such events (see the Incident Management section below).

To maintain the integrity and confidentiality of communications, GDC connected utilizes the Transport Layer Security (TLS) protocol to provide communication security over data transmissions between the GCP production environment and external users.

Mobile Device Management

Google has 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.

Endpoints are laptops and desktops used by GDC connected employees that may have access to interact with the GCP production environment. Accordingly, these systems require the appropriate level of safeguards against potential threats. IT is responsible for GDC connected 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, GDC connected 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.

Authentication, Authorization, and Administration

Strong authentication and access controls are implemented to restrict access to GDC connected production systems, internal support tools, and customer data. Machine-level access restriction relies on a Google-developed distributed authentication service, based on 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 used by Google operational staff to maintain and troubleshoot the systems for GDC connected 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 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 certificates. Periodic reviews of access lists are implemented to help ensure that access to customer data (and other need-to-know data) is appropriate and authorized. Access to production machines, network devices, and support tools is managed via an access group management system. Membership in these groups must be approved by respective group administrators. User group memberships are reviewed semiannually under the direction of the group administrators to ensure that access has been removed for employees who no longer have a business need for such access.

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

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 at least annually.

Access to the customer's GDC connected application occurs via a web browser. The Support Access feature is limited to approved GDC connected employees based on job responsibilities and requires two-factor authentication via username, password, and authentication application. Customers can disable or grant specific time limits to the Support Access feature through a product configuration.

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

- Configuration management tool – GDC connected 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.

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 GDC connected 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 GDC connected 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 is independent of the developer assigned and follow 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 are subject to additional review. Software ready for deployment to production 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 the functionality of internal tools that support the build and release process.

Tools are also utilized to detect deviations from pre-defined 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.

External third-party penetration tests are performed annually for a predetermined subset of the services included in GDC connected, 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 Company's current risk environment, as well as the 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 24/7. 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 determine 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. 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 and 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 the notifying of 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 personnel via pager. The escalation time and contacts are defined in the escalation tool configuration files. This leads to automatic 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 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 has a 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. Google maintains defined terms regarding the return, transfer, and disposal of user data and makes these terms available to customers.

By default, the GDC connected cache is refreshed at least every 30 days, ensuring that customer query results do not persist within the GDC connected environment past that time period. GDC connected 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 GDC connected, this initiates an automated process that deletes the relevant customer data, including the customer's GDC connected configuration, usernames and passwords, database connection information, GKE instances, and internal databases within 30 days, as well as related backup information within one year.

Backup and Recovery

GDC connected has a defined 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, GDC connected application data is backed up every 24 hours to GCP for further redundancy. Backups are encrypted before being transmitted, and access to backups is restricted to administrators. Administrators can configure their GDC connected instances to use different backup settings or a different destination for backups.

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. GDC connected conducts restoration tests annually. Results from these tests are recorded and reviewed regularly.

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 that document the results and lessons learned from the tests.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the API, the customer or end-user defines and controls the data they load into and store in the GDC connected production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest. The following table details the types of data contained in the production application for GDC connected:

Data		
Production Application	**Description**	**Data Store**
Google Operational Data	Google Operational Data is required for Google to ensure that GDC connected performs as expected and to proactively provide support. The operational data generally consists of the platform configuration parameters, performance metrics, and status logging. Google's operational data is encrypted in transit using MASQUE VPN (a Google-developed QUIC-based VPN	Rack management and Point of Presence (PoP) datastores in Google production environments, encrypted at rest.

Data		
Production Application	**Description**	**Data Store**
	technology) and TLS. Google operational data is encrypted at rest using standard Linux disk encryption in accordance with Google's internal requirements for such data. Google operational data is transmitted to Google's production infrastructure and stored and analyzed using Google's internally developed tools. Data generated on GDC connected systems is proprietary, both in content and format. However, relevant infrastructure data about on-premises GDC connected racks used by a customer as part of GDC connected services, such as high-level hardware system conditions or resource consumption, is exposed to the customer via standard Google Cloud Operations.	
Customer Operational Data	Customer operational data is the set of information that is used to configure the workloads for delivery of application services and non-application data generated during the execution of that workload by GDC connected. This operational data can be further characterized as one of two types. Configuration data consumed by components of GDC connected to manage their Kubernetes Cluster on-prem. (e.g., network configuration, boot time Customer-Managed Encryption Keys [CMEK]). This data is encrypted in transit with HTTPS, except for the GDC connected network API (edgenetwork.googleapis.com), which is carried over MASQUE VPN. Data generated by the application workloads that is not consumed by GDC connected components (e.g., application workload configuration). This includes any configuration information that is consumed only by the application workload itself and any monitoring data or logs generated by the application workload.	Stored on GCP in a customer project, encrypted at rest by GCP, with customer managed encryption available.
Customer Workload and Application Data	The application data is data generated by the client's application: content, such as IP traffic, voice, control data, and traffic data of the session, but also metadata, such as connection status, location, authentication, and billing records. By design the application data is not gathered, exported, or analyzed by Google systems. GDC connected encrypts all data at rest. When a customer elects to use CMEKs, the data at rest is encrypted using keys managed by the client, and encryption in transit is a function of the application workloads configured by the client.	Stored on the GDC connected data disk double encrypted with Linux Unified Key Setup (LUKS) and self-encrypting drive (SED).

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.

Log files may contain sensitive information. To ensure log privacy and integrity, GDC connected maintains a centralized logging solution to protect this information from unauthorized disclosure and manipulation.

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.
- GDC connected 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 the importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk tend to be evaluated more often.

Evaluations often take the form of self-assessments, in which personnel responsible for a particular unit or function determine the effectiveness of controls for their activities. These assessments are considered by management, along with any other internal control evaluations. The findings of these efforts are utilized to ensure that follow-up actions are taken, and subsequent evaluations are modified as necessary. 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 Google'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.

Availability

The availability category refers to the accessibility of the system or services as committed by Google's Terms of Service. GDC connected'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, 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 telecommunications 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) the 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.

User Entity Responsibilities

Management of user entities is responsible for the following, which should not be regarded as a comprehensive list of all controls that should be employed by user entities:

- 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
- 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.
- User entities should 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.
- User entities should 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)

GDC connected uses GCP for cloud hosting services. Google's controls related to GDC connected cover only a portion of the overall internal control for each user entity of GDC connected. The description does not extend to the controls of GCP. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of Google's GDC connected service and exclude the related controls of GCP, which are covered via GCP reporting.

Although the complementary subservice organization controls of Google have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by GCP.

For example, GCP's controls that are expected to be in place include physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. GCP's physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

For the GDC connected service, Google management receives and reviews the GCP SOC 2 report annually. Management monitors the services performed to determine whether operations and controls

expected to be implemented are functioning effectively. Management also communicates within the organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to GCP management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to GDC connected to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with Google's controls related to GDC connected and related tests and results described in Section 4 of this report, considering the related subservice organization controls expected to be covered via GCP reporting as described below.

Criteria	Complementary Subservice Organization Controls
CC2.3	• Inspecting the Vendor Audit Reports as determined by the sensitivity of data being processed or access being granted.
CC6.4	• Restricting data center access to authorized personnel. • 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC9.2	• Inspecting Vendor Risk Assessments for security and privacy risks for all cloud subprocessors annually.
CC7.2 A1.2	• Installation of fire suppression and detection and environmental monitoring systems at the data centers. • Protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • 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*), in AICPA, *Trust Services Criteria* 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 GDC connected was used to provide the service from November 1, 2023 to October 31, 2024.

Report Use

The description does not omit or distort information relevant to GDC connected 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, 2023 to October 31, 2024. In selecting particular tests of the operating effectiveness of the controls, we considered (i) the nature of the controls being tested; (ii) the types of available evidential matter; (iii) the nature of the criteria to be achieved; (iv) the assessed level of control risk; and (v) the expected efficiency and effectiveness of the test. Such tests were used to evaluate fairness of the presentation of the description of Google's Google Distributed Cloud (GDC) connected 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, Data Security Policy, and Security and Resilience Policy to determine that the organization had established internal privacy and information security policies, as well as a Code of Conduct, that were reviewed and updated as needed.	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 hire employees, temporary workers, and independent contractors to determine that employees and members of the extended workforce were required to acknowledge the Code of Conduct upon hire.	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 employees, temporary workers, and independent contractors, in compliance with local laws, upon hire.	No exceptions noted.
		Inspected background check documentation for a sample of new employees, temporary workers, and independent contractors to determine that background checks were performed as required for all new members of the organization, in compliance with 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**
	The organization establishes confidentiality agreements with extended workforce personnel to define responsibilities and expected behavior for the protection of information.	Inspected the confidentiality agreement template to determine that the organization had established confidentiality agreements with 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 extended workforce personnel to determine that extended workforce personnel acknowledged the organization's established confidentiality agreements, which 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 and Code of Conduct to determine that the organization 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 organization'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**
	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 and the internal case management system to determine that the organization 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 organization enforced a disciplinary process to address non-compliance with Company policies, the Code of Conduct, or other personnel requirements.	No exceptions noted.
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. 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 Corporate Governance Guidelines and an example board meeting calendar invite and agenda to determine that all board members exercised independent judgment, with independent/non-employee directors demonstrating independence from management in exercising oversight of internal control.	No exceptions noted.
		Inspected the Corporate Governance Guidelines and the board listing on the Investor Relations webpage to determine that the board demonstrated independence from management.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
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 organization had implemented a formal reporting structure that was made available to personnel.	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 Security organizational charts to determine that information security was managed by a dedicated executive, independent of Information Technology (IT) responsibility, with authority to escalate security issues to the board level as needed.	No exceptions noted.
		Inspected an example meeting calendar invite and agenda for a recent Security and Privacy team meeting to determine that a Security executive met with relevant personnel to discuss security issues and had the option to escalate concerns to the board level as needed.	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**
	All board of directors exercise independent judgment. 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 Corporate Governance Guidelines and an example board meeting calendar invite and agenda to determine that all board members exercised independent judgment, with independent/non-employee directors demonstrating independence from management in exercising oversight of internal control.	No exceptions noted.
		Inspected the Corporate Governance Guidelines and the board listing on the Investor Relations webpage to determine that the board demonstrated independence from management.	No exceptions noted.
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, Basic Security 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 that 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 configurations for the automated training enrollment tool, and an example of an email notification sent to employees for overdue training to determine that the organization had established a privacy and information security training program and that relevant personnel met the requirement to complete the training annually.	No exceptions noted.

Control Environment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the security awareness training content to determine that security awareness training content was reviewed and updated at least 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.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
	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 hire employees, temporary workers, and independent contractors to determine that employees and members of the extended workforce were required to acknowledge the Code of Conduct 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 and the internal case management system to determine that the organization 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 organization enforced a disciplinary process to address non-compliance with Company policies, the Code of Conduct, or other personnel requirements.	No exceptions noted.

Control Environment			
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.

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 organization established an Internal Audit function which evaluated management's compliance with security controls at least annually.	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 continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
		Inspected audit log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
		Inspected monitoring dashboards, alert threshold configurations, and example alerts to determine that alerts were generated for further investigation.	No exceptions noted.
	The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Inspected the Security Logging Policy, Vulnerability Management Guidelines, Vulnerability Severity Guidelines, and alerting configurations to determine that policies and protection mechanisms were documented and configured for detecting and reporting operational issues.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected monitoring tool dashboards, alerting configurations, and an example alert to determine that monitoring tools were provided to personnel for detecting and reporting operational issues.	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 organization 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 vulnerability scanning frequency configurations, a sample of monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.
		Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The organization periodically reviews and validates the design, operation and control record of in-scope compliance controls.	Inspected tickets and documentation of the organization's risk assessment evaluations to determine that the organization reviewed and validated the design, operation, and control record of in-scope compliance controls at least annually and that corrective actions were taken based on relevant findings.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
	The descriptions of the Company's systems (including their scope and boundaries) are made available to internal teams.	Inspected the Company's intranet to determine that GDC connected's product description (including scope and boundaries) was made available to internal teams.	No exceptions noted.
	The organization has policies addressing confidentiality, integrity, and availability that have been approved and made available to internal teams.	Inspected the organization's security policies and procedures to determine that they addressed security, confidentiality, and availability and had been approved by management.	No exceptions noted.
		Inspected the organization's intranet accessible to all employees to determine that the organization had policies addressing security, confidentiality, and availability that had been communicated to employees.	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 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**
		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 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 organization's security policies and procedures to determine that the organization 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 organization managed operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly supported the operation of the organization's products and services.	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 organization had established an incident response policy that was reviewed annually and outlined management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents, which were categorized by severity.	No exceptions noted.

Information and Communication			
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 Security organizational charts to determine that information security was managed by a dedicated executive, independent of Information Technology (IT) responsibility, with authority to escalate security issues to the board level as needed.	No exceptions noted.
		Inspected an example meeting calendar invite and agenda for a recent Security and Privacy team meeting to determine that a Security executive met with relevant personnel to discuss security issues and had the option to escalate concerns to the board level as needed.	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 Cloud Data Processing Addendum (CDPA), Service Level Objectives (SLO), and the GDCE Terms of Service (ToS).	Inspected the Cloud Data Processing Addendum (CDPA), Service Level Objectives (SLO), and the GDCE ToS to determine that the organization's commitments to security, availability, and confidentiality were communicated to external users via publications such as the CDPA, SLO, and ToS.	No exceptions noted.
	The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Inspected the nondisclosure agreement (NDA) templates to determine that the organization's agreements, including NDAs, provided details on preserving confidentiality of information and software exchanges.	No exceptions noted.
		Inspected the Google Cloud Platform ToS to determine that the organization established agreements for preserving confidentiality of information and software exchanges with external parties.	No exceptions noted.

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	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 vendors/service providers and partners, respectively.	Inspected the CDPA template to determine that the organization required external parties (Service Providers) to meet security & privacy requirements for safeguarding user data and that requirements were enforced via the "Information Protection Addendum (IPA)" or the "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.	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 in-scope systems to determine that the organization had implemented a contractual addendum 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 organization's obligations regarding customer data.	No exceptions noted.
	The Privacy, Safety Security Org (PSS) 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. A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the	Inspected the Vendor Security Assessment Guidelines to determine that the PSS Org had a documented, risk-based approach to reviewing the security practices of vendors and the security posture of vendor products.	No exceptions noted.
		Inquired of management and inspected the population of third-party vendors and subprocessors to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether both automated and	Not tested. There were no applicable external parties employed by GDC

Information and Communication			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	period. There were no applicable external parties employed by GDC connected during the period.	manual assessments were performed based on data sensitivity.	connected during the period.
	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 organization 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 Distributed Cloud connected product information on the Company's publicly available website to determine that descriptions of the Company's system and its boundaries were available to authorized external users via ongoing communications with customers or via its official blog postings.	No exceptions noted.
	Customer responsibilities are described on the organization's product websites or in system documentation.	Inspected Company product websites, system documentation, the GDC connected Terms of Service (ToS), and the Google CDPA to determine that customer responsibilities were described on the Company's product websites and in system documentation.	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 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.

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.		
	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 organization 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 management of the organization evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	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 conducts periodic Information Security Risk Assessments to identify and evaluate risks.	Inspected the risk assessment performed for in-scope systems to determine that the organization conducted an Information Security Risk Assessment to identify and evaluate risks.	No exceptions noted.
		Inspected the risk assessment documentation to determine that the organization's risk assessment considered the 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**
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 maintains a framework that defines how to organize a response to security & privacy incidents.	Inspected internal incident response webpages and Security Incident Response Team processes within the Information Security and Privacy Incident Response Policy to determine that a framework was in place for organizing a response to security and 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 Disaster Resiliency (DR) and Business Continuity (BC) planning documentation and testing checklists to determine that DR and BC testing was required to be conducted at least annually and included communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.
		Inspected DR and BC testing documentation and results to determine that the organization 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 conducts periodic Information Security Risk Assessments to identify and evaluate risks.	Inspected the risk assessment performed for in-scope systems to determine that the organization conducted an Information Security Risk Assessment to identify and evaluate risks.	No exceptions noted.

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the risk assessment documentation to determine that the organization's risk assessment considered the 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.
	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 organization 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 management of the organization evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	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.
CC3.3	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 organization developed and maintained a risk management framework to manage risk to an acceptable level.	No exceptions noted.

Risk Assessment			
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 management of the organization 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 organization conducted an Information Security Risk Assessment to identify and evaluate risks.	No exceptions noted.
		Inspected the risk assessment documentation to determine that the organization's risk assessment considered the 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.
	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 using a methodology / frequency aligned with compliance requirements and customer commitments. Corrective actions are taken in accordance with vulnerability management processes. A portion of the control did not operate during the period because the circumstances that warrant the	Inspected the annual penetration test results to determine that penetration tests were performed at least annually, using a methodology / frequency which aligned with compliance requirements and customer commitments.	No exceptions noted.
		Inquired of management and inspected the penetration test report to determine that the circumstances that warrant the	Not tested. No corrective actions

Risk Assessment			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	operation of the control did not occur during the period. No corrective actions were required during the period.	operation of the control did not occur during the period. As a result, no testing could be performed to determine whether 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.	were required during the period.
	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 organization 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 management of the organization 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 organization conducted an Information Security Risk Assessment to identify and evaluate risks.	No exceptions noted.
		Inspected the risk assessment documentation to determine that the organization's risk assessment considered the 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**
	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.

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 periodically reviews and validates the design, operation and control record of in-scope compliance controls.	Inspected tickets and documentation of the organization's risk assessment evaluations to determine that the organization reviewed and validated the design, operation, and control record of in-scope compliance controls at least annually and that corrective actions were taken based on relevant findings.	No exceptions noted.
	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 organization established an Internal Audit function which evaluated management's compliance with security controls at least annually.	No exceptions noted.
	Penetration tests are performed using a methodology / frequency aligned with compliance requirements and customer commitments. Corrective actions are taken in accordance with vulnerability management processes. A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No corrective actions were required during the period.	Inspected the annual penetration test results to determine that penetration tests were performed at least annually, using a methodology / frequency which aligned with compliance requirements and customer commitments.	No exceptions noted.
		Inquired of management and inspected the penetration test report to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether 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.	Not tested. No corrective actions were required during the period.

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 organization 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 vulnerability scanning frequency configurations, a sample of monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.
		Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	No exceptions noted.
	The Privacy, Safety Security Org (PSS) 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. A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. There were no applicable external parties employed by GDC connected during the period.	Inspected the Vendor Security Assessment Guidelines to determine that the PSS Org had a documented, risk-based approach to reviewing the security practices of vendors and the security posture of vendor products.	No exceptions noted.
		Inquired of management and inspected the population of third-party vendors and subprocessors to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether both automated and manual assessments were performed based on data sensitivity.	Not tested. There were no applicable external parties employed by GDC connected during the period.

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 organization established an Internal Audit function which evaluated management's compliance with security controls at least annually.	No exceptions noted.
	The Privacy, Safety Security Org (PSS) 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. A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. There were no applicable external parties employed by GDC connected during the period.	Inspected the Vendor Security Assessment Guidelines to determine that the PSS Org had a documented, risk-based approach to reviewing the security practices of vendors and the security posture of vendor products.	No exceptions noted.
		Inquired of management and inspected the population of third-party vendors and subprocessors to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether both automated and manual assessments were performed based on data sensitivity.	Not tested. There were no applicable external parties employed by GDC connected during the period.
	The organization periodically reviews and validates the design, operation and control record of in-scope compliance controls.	Inspected tickets and documentation of the organization's risk assessment evaluations to determine that the organization reviewed and validated the design, operation, and control record of in-scope compliance 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 organization 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 vulnerability scanning frequency configurations, a sample of monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.
		Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
	The 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 to determine that an internal audit function was in place and that the organization regularly engaged independent third parties to review the effectiveness of the organization's information security and privacy practices, with findings and corrective actions tracked and communicated to stakeholders.	No exceptions noted.
		Inspected security compliance certifications from independent audits to determine that the organization regularly engaged third parties for independent reviews of its information security practices.	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 organization 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 management of the organization 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 organization conducted an Information Security Risk Assessment to identify and evaluate risks.	No exceptions noted.
		Inspected the risk assessment documentation to determine that the organization's risk assessment considered the 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.
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 organization 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 management of the organization 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 to determine that an internal audit function was in place and that the organization regularly engaged independent third parties to review the effectiveness of the organization's information security and privacy practices, with findings and corrective actions tracked and communicated to stakeholders.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected security compliance certifications from independent audits to determine that the organization regularly engaged third parties for independent reviews of its information security practices.	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 conducts periodic Information Security Risk Assessments to identify and evaluate risks.	Inspected the risk assessment performed for in-scope systems to determine that the organization conducted an Information Security Risk Assessment to identify and evaluate risks.	No exceptions noted.
		Inspected the risk assessment documentation to determine that the organization's risk assessment considered the 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.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
	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 incident reporting settings on the intranet to determine that the organization provided internal personnel (employees & extended workforce) with instructions and mechanisms for reporting potential security & privacy concerns or incidents to the responsible team(s).	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Security and privacy policies are reviewed at least annually. Supporting standards, guidelines, and FAQs are created and updated as needed.	Inspected the organization's security and privacy policies, supporting standards, guidelines, and FAQs to determine that security and privacy policies were reviewed at least annually and that supporting standards, guidelines, and FAQs were created and updated as needed.	No exceptions noted.
	The organization has policies and guidelines that govern third-party relationships.	Inspected the Google VSA Guidelines and support tool dashboards to determine that policies and procedures were developed to govern 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 Guidelines, and the Security Requirements for Outsourced Software Development Policy to determine that the organization had established policies and guidelines governing the secure development lifecycle, including outsourced development.	No exceptions noted.
	The organization has change management policies and guidelines in place for tracking, testing, approving, and validating changes, including security code reviews.	Inspected the Change Management Security Policy and secure coding guidelines to determine that policies and guidelines for tracking, testing, approving, and validating changes, including security code reviews, were in place.	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. A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No data deletions occurred during the period.	Inspected the Data Destruction Guidelines and User Data Wipeout Policy to determine that the organization had procedures in place to dispose of confidential and ntk information in accordance with the data retention and deletion policy.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inquired of management and inspected data deletion documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether the organization implemented procedures to dispose of confidential information according to the data retention and deletion policy.	Not tested. No data deletions occurred during the period.
	The organization maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers.	Inspected the organization's CDPA, the Data Processing and Security Terms (DPST), and the GDC connected Service Terms on the publicly available Company website to determine that the organization maintained policies regarding the return, transfer, and disposal of user data and made these policies available to customers.	No exceptions noted.
	The organization has policies and guidelines that govern the acceptable use of information assets.	Inspected the Data Security Policy, the Data Classification Guidelines and procedures, and the Code of Conduct to determine that the organization had established policies and procedures that governed the acceptable use of information assets.	No exceptions noted.
	The organization has established policies and guidelines to govern data classification, labeling and security.	Inspected the GDCE Service Terms, the CDPA, and the DPST to determine that the Company established policies and guidelines to define customer data and govern data classification, labeling, and security.	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 Account Security Policy and 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.

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 organization 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 vulnerability scanning frequency configurations, a sample of monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.
		Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	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 organization had established an incident response policy that was reviewed annually and outlined management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents, which were categorized by severity.	No exceptions noted.

Control Activities			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	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 organization's security policies and procedures to determine that the organization 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 organization managed operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly supported the operation of the organization's products and services.	No exceptions noted.
	The organization has policies addressing confidentiality, integrity, and availability that have been approved and made available to internal teams.	Inspected the organization's security policies and procedures to determine that they addressed security, confidentiality, and availability and had been approved by management.	No exceptions noted.
		Inspected the organization's intranet accessible to all employees to determine that the organization had policies addressing security, confidentiality, and availability that had been 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 organization 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 management of the organization evaluated risks by defining risk ratings and considered the risk of engaging with third parties.	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 organization's Cryptographic Policy to determine that guidelines were in place for protecting against teleworking risks and required encrypted communication systems for remote access.	No exceptions noted.
		Inspected the encryption configuration for remote authentication to determine that users accessed the system exclusively through 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 organization's Certificate Authority Policy and the Account Authentication Guidelines to determine that remote access to corporate machines required a digital certificate issued by the organization 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.
		Inspected authentication configurations for remote access to corporate machines to determine that a digital certificate issued by the organization installed on the connecting device, along with two-factor authentication (user ID, password, security key, and/or certificate), was required for remote access.	No exceptions noted.
	The organization has an established key management process in place to support the organization's use of cryptographic techniques.	Inspected the Cryptographic Policy and Key Management Policy to determine that an established key management process was in place to support the organization's use of cryptographic techniques.	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 code configuration for enforcing encryption, certificate authentication, and revocation to determine that an established key management process supported the organization'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 required a unique ID, password, and/or machine certificate.	No exceptions noted.
		Inspected network timeout configurations to determine that active certificates expired and network sessions were automatically timed out after 20 hours of inactivity.	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 enforcing user authentication prior to granting private key access to determine that only users with a valid user certificate, corresponding private key, and host-specific authorization could access production machines via Secure Shell (SSH).	No exceptions noted.
		Inspected the configuration enforcing key-based authentication to determine that SSH access to production machines was restricted to authorized users with valid digital certificates.	No exceptions noted.
	Logical access to organization owned network devices is authenticated via user ID, password, security key, and/or certificate.	Inspected the authentication configuration enforcing user IDs, passwords, security keys, and/or valid certificates to determine that logical access to organization-owned network devices was authenticated through enforced methods.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	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 required two-factor authentication using a distinct user ID, password, and a security key or certificate.	No exceptions noted.
		Inspected the code enforcing user authentication prior to certificate issuance to determine that personnel access to sensitive internal systems and applications required two-factor authentication with a distinct user ID, password, and security key or certificate and that certificates were generated only after successful two-factor authentication for single sign-on.	No exceptions noted.
	External system users are identified and authenticated via the Google Accounts or the BYOID authentication system before access is granted.	Inspected the configuration used to identify and authenticate external system users via Google Accounts or the Bring Your Own Identity (BYOID) authentication system to determine that users were identified and authenticated before being granted access to cloud services.	No exceptions noted.
		Inspected the customer account creation process to determine that external system users created their own passwords and were identified and authenticated via Google Accounts or the BYOID authentication system before accessing cloud services.	No exceptions noted.
	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 formal guidelines for passwords were established to govern the management and use of authentication mechanisms.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected SSH idle time configurations on servers to determine that they were configured to enforce password requirements according to formal authentication guidelines.	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 formal guidelines for managing authentication mechanisms.	No exceptions noted.
		Inspected the authentication configurations to determine that passwords were transmitted and stored using encrypted procedures according to formal password management guidelines.	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 network architecture and segmentation requirements within the Company's network diagrams and Network Access Security Policies to determine that the Company segmented networks based on the nature of services, users, and information systems that were being accessed.	No exceptions noted.
		Inspected the connection pathways of an example network within the network device monitoring tool and the configuration for access control and authentication requirements for production network access to determine that networks were segmented based on the nature of services, users, and information systems that were being accessed.	No exceptions noted.

Logical and Physical Access Controls			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Customer data that is uploaded or created is encrypted at rest.	Inspected the organization's Cryptographic Policy and default encryption-at-rest webpage to determine that customer data uploaded or created was required to be encrypted at rest according to storage-level encryption requirements.	No exceptions noted.
		Inspected data backup encryption configurations and encryption settings for storage devices containing customer data to determine that uploaded and created customer data was encrypted at rest.	No exceptions noted.
	The organization maintains an up-to-date, accurate client device inventory.	Inspected the procedures for inventorying client assets and a system-generated list of assets to determine that the organization maintained an up-to-date, accurate client device inventory.	No exceptions noted.
	Access to internal support tools is restricted to authorized personnel through the use of approved credentials.	Inspected TLS protocol configurations and the enforcement of two-factor authentication (user ID with password, security key, and/or certificate) to determine that access to internal support tools was restricted to authorized personnel using approved credentials.	No exceptions noted.
		Inspected semi-annual critical access group membership review evidence, a sample of critical access group members, and their job titles to determine that access to internal support tools was restricted to authorized personnel using approved credentials.	No exceptions noted.
	Encryption is used to protect user authentication and administrator sessions transmitted over the Internet.	Inspected the organization's Cryptographic Policy and the CDPA webpage available to external users to determine that encryption mechanisms were required and communicated to protect user authentication and administrator sessions transmitted over the Internet.	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 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 firewall and network configurations, and an example alert, to determine that mechanisms detected and prevented unauthorized devices from connecting to the organization's network.	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 system, rollback procedures, Change Management Security Policy, and CDPA to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions and that safeguards were provided to ensure the integrity and availability of cloud customer data during system restorations.	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 organization used the version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.
		Inspected evidence from the annual critical access group membership review, including a sample of users with access to the version control system and their respective job titles, to determine that access was reviewed and approved through the annual review process.	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 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 Account Security Policy and 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.
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.
		Inspected the access control management tool history log, tool configuration, and examples of a new hire and transferred employee to determine that modifications to access control lists were recorded and approved by administrators.	No exceptions noted.
	Access to production machines, support tools, network devices and corporate assets is automatically removed in a timely basis upon submission of a termination request by Human Resources or a manager.	Inspected the Identity and Access Management Policy to determine that the organization documented procedures for terminating user access to production machines, support tools, network devices, and corporate 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**
		Inspected the configuration of the automated tool used to revoke access to production machines, support tools, network devices, and corporate assets to determine that access was configured to be automatically removed 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 to determine that access to production machines, support tools, network devices, and corporate assets was automatically removed in a timely manner using the automated tool 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' configuration to determine that reviews were assigned to authorized group administrators, ensuring that logical access was restricted to authorized personnel and reviewed at least semi-annually.	No exceptions noted.
		Inspected critical access group user membership reviews performed by group administrators to determine that critical access group memberships were reviewed at least semi-annually to ensure that access was restricted appropriately and that reviews were tracked to completion.	No exceptions noted.
		Inspected automatic account revocation configurations to determine that inappropriate access identified during the semi-annual critical access group membership reviews was removed at least hourly.	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 separates duties of individuals by granting users access based on job responsibilities and least privilege, and limiting access to only authorized users.	Inspected the Identity and Access Management Policy to determine that the organization separated duties by granting users access based on job responsibilities and least privilege by limiting access to only authorized users.	No exceptions noted.
		Observed an attempt to access a privileged system outside the user's job responsibilities to determine that the organization's separation of duties and principle of least privilege successfully limited access to authorized users only.	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.
		Inspected the access control management tool history log, tool configuration, and examples of a new hire and transferred employee to determine 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 organization documented procedures for terminating user 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 access was configured to be automatically removed 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 to determine that access to production machines, support tools, network devices, and corporate assets was automatically removed in a timely manner using the automated tool 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' configuration to determine that reviews were assigned to authorized group administrators, ensuring that logical access was restricted to authorized personnel and reviewed at least semi-annually.	No exceptions noted.
		Inspected critical access group user membership reviews performed by group administrators to determine that critical access group memberships were reviewed at least semi-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**
		Inspected automatic account revocation configurations to determine that inappropriate access identified during the semi-annual critical access group membership reviews was removed at least hourly.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
	The Company utilizes a third-party contractor to host, maintain, and protect production servers, network devices, and network connections in data centers. The third-party data centers that host information assets are carved out for the purposes of this report.	Not applicable.	Not applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.		
	The organization sanitizes storage media prior to disposal, release from organizational control, or release for reuse.	Inspected policies and guidelines to determine that the organization was required to sanitize storage media prior to disposal, release from organizational 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. A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No data deletions occurred during the period.	Inspected the Data Destruction Guidelines and User Data Wipeout Policy to determine that the organization had procedures in place to dispose of confidential and ntk information in accordance with 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**
		Inquired of management and inspected data deletion documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether the organization implemented procedures to dispose of confidential information according to the data retention and deletion policy.	Not tested. No data deletions occurred during the period.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
	The organization has implemented perimeter devices to protect the corporate network from external network attacks.	Inspected policies, design documentation, network topology diagrams, and firewall and global router configurations to determine that perimeter devices were implemented to protect the corporate network from external attacks.	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 organization's Certificate Authority Policy and the Account Authentication Guidelines to determine that remote access to corporate machines required a digital certificate issued by the organization 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.
		Inspected authentication configurations for remote access to corporate machines to determine that a digital certificate issued by the organization installed on the connecting device, along with two-factor authentication (user ID, password, security key, and/or certificate), was required for remote access.	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 used to protect user authentication and administrator sessions transmitted over the Internet.	Inspected the organization's Cryptographic Policy and the CDPA webpage available to external users to determine that encryption mechanisms were required and communicated to protect user authentication and administrator sessions transmitted over the Internet.	No exceptions noted.
		Inspected configurations around encryption mechanisms to determine that user authentication and administrator sessions transmitted over the internet were encrypted.	No exceptions noted.
	Mechanisms are in place to detect attempts, and prevent connections to the organization's network by unauthorized devices.	Inspected firewall and network configurations, and an example alert, to determine that mechanisms detected and prevented unauthorized devices from connecting to the organization's network.	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 continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
		Inspected audit log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
		Inspected monitoring dashboards, alert threshold configurations, and example alerts to determine that alerts were generated for further investigation.	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 maintains policies that define the requirements for the use of cryptography.	Inspected the organization's Cryptographic Policy and Account Authentication Security Guidelines to determine that policies were in place defining cryptography requirements.	No exceptions noted.
	The organization maintains policies and guidelines for securing mobile devices used to access corporate networks and systems.	Inspected the Mobile Device Support Policy and Mobile Device Security Guidelines to determine that the organization maintained policies and guidelines for securing mobile devices used to access the corporate networks and systems.	No exceptions noted.
	The organization prohibits the use of removable media for the storage of PII and SPII unless the data has been encrypted.	Inspected the Data Security Policy, Removable Media documentation, and the organization's Cryptographic Guidelines to determine that the use of removable media for storing Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII) was prohibited unless the data was encrypted.	No exceptions noted.
	The organization has established guidelines for governing the installation of software on organization-owned assets.	Inspected the Third-Party Software Installation Security Guidelines to determine that guidelines were established to govern software installation on organization-owned assets.	No exceptions noted.
	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 organization's Cryptographic Policy to determine that guidelines were in place for protecting against teleworking risks and required encrypted communication systems for remote access.	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 encryption configuration for remote authentication to determine that users accessed the system exclusively through encrypted communication systems.	No exceptions noted.
	Encryption is used to protect user authentication and administrator sessions transmitted over the Internet.	Inspected the organization's Cryptographic Policy and the CDPA webpage available to external users to determine that encryption mechanisms were required and communicated to protect user authentication and administrator sessions transmitted over the Internet.	No exceptions noted.
		Inspected configurations around encryption mechanisms to determine that user authentication and administrator sessions transmitted over the internet were encrypted.	No exceptions noted.
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 Vulnerability Management and System Security Policies and Guidelines to determine that antivirus, antimalware, antispam, and antiphishing tools were implemented and that technical measures were in place to securely configure, monitor, and protect customer and Google cloud administration management consoles and 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 organization'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 and Device Configuration Guidelines to determine that monitoring tools were documented to send automated alerts to operational personnel based on predetermined criteria, with incidents escalated per policy.	No exceptions noted.
		Inspected alert configurations and an example alert sent from monitoring tools to operational personnel to determine that automated alerts were sent based on predetermined criteria, with incidents 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 Security Logging Policy, Vulnerability Management Guidelines, Vulnerability Severity Guidelines, and alerting configurations to determine that policies and protection mechanisms were documented and configured for detecting and reporting operational issues.	No exceptions noted.
		Inspected monitoring tool dashboards, alerting configurations, and an example alert to determine that monitoring tools were provided to personnel for detecting and reporting 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 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 organization's resource management documentation to determine that procedures related to managing information processing resources were made available and included guidance on requesting, monitoring, and maintaining resources, as well as forecasting capacity requirements to identify usage trends and manage system overload.	No exceptions noted.
	The organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting based on usage and system performance.	Inspected the resource management policies and procedures to determine that the capacity of the organization's information processing resources was managed through a combination of planning, monitoring, and adjusting based on usage and system performance.	No exceptions noted.
		Inspected the internal capacity monitoring dashboards to determine that the organization managed the capacity of its information processing resources through a combination of planning, monitoring, and adjusting based on usage and system performance.	No exceptions noted.
		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**
	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 organization 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 vulnerability scanning frequency configurations, a sample of monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.
		Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	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 organization conducted an Information Security Risk Assessment to identify and evaluate risks.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected the risk assessment documentation to determine that the organization's risk assessment considered the 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.
	The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Inspected the Security Logging Policy, Vulnerability Management Guidelines, Vulnerability Severity Guidelines, and alerting configurations to determine that policies and protection mechanisms were documented and configured for detecting and reporting operational issues.	No exceptions noted.
		Inspected monitoring tool dashboards, alerting configurations, and an example alert to determine that monitoring tools were provided to personnel for detecting and reporting operational issues.	No exceptions noted.
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.		
	The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.	Inspected the Security Logging Policy, Vulnerability Management Guidelines, Vulnerability Severity Guidelines, and alerting configurations to determine that policies and protection mechanisms were documented and configured for detecting and reporting operational issues.	No exceptions noted.
		Inspected monitoring tool dashboards, alerting configurations, and an example alert to determine that monitoring tools were provided to personnel for detecting and reporting operational issues.	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 webpages and Security Incident Response Team processes within the Information Security and Privacy Incident Response Policy to determine that a framework was in place for organizing a response to security and privacy incidents.	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 and Device Configuration Guidelines to determine that monitoring tools were documented to send automated alerts to operational personnel based on predetermined criteria, with incidents escalated per policy.	No exceptions noted.
		Inspected alert configurations and an example alert sent from monitoring tools to operational personnel to determine that automated alerts were sent based on predetermined criteria, with incidents escalated per policy.	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 continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
		Inspected audit log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
		Inspected monitoring dashboards, alert threshold configurations, and example alerts to determine that alerts were generated for further investigation.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Penetration tests are performed using a methodology / frequency aligned with compliance requirements and customer commitments. Corrective actions are taken in accordance with vulnerability management processes. A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No corrective actions were required during the period.	Inspected the annual penetration test results to determine that penetration tests were performed at least annually, using a methodology / frequency which aligned with compliance requirements and customer commitments.	No exceptions noted.
		Inquired of management and inspected the penetration test report to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether 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.	Not tested. No corrective actions were required during the period.
	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 organization 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 vulnerability scanning frequency configurations, a sample of monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	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 organization's resource management documentation to determine that procedures related to managing information processing resources were made available and included guidance on requesting, monitoring, and maintaining resources, as well as forecasting capacity requirements to identify usage trends and manage system overload.	No exceptions noted.
	The organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting based on usage and system performance.	Inspected the resource management policies and procedures to determine that the capacity of the organization's information processing resources was managed through a combination of planning, monitoring, and adjusting based on usage and system performance.	No exceptions noted.
		Inspected the internal capacity monitoring dashboards to determine that the organization managed the capacity of its information processing resources through a combination of planning, monitoring, and adjusting based on usage and system performance.	No exceptions noted.
		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.		
	Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inspected the Information Security and Privacy Incident Response Policy to determine that information security incidents were required to be documented per the organization's Incident Response Policy.	No exceptions noted.
		Inspected the root cause analysis and remediation documentation for a sample of security event and incident tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents were used to strengthen and improve security controls, prevent future incidents, and could be used as examples for information security training.	No exceptions noted.
		Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated for potential impact on security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.
		Inspected a sample of security incident tickets to determine that security incidents were logged, tracked, resolved, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	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 organization maintained internal policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	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 continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
		Inspected audit log configurations and example audit logs to determine that audit logs were continuously monitored for events related to security, availability, and confidentiality threats and that alerts were generated for further investigation.	No exceptions noted.
		Inspected monitoring dashboards, alert threshold configurations, and example alerts to determine that alerts were generated for further investigation.	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 organization had established an incident response policy that was reviewed annually and outlined management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents, which were categorized by severity.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Penetration tests are performed using a methodology / frequency aligned with compliance requirements and customer commitments. Corrective actions are taken in accordance with vulnerability management processes. A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No corrective actions were required during the period.	Inspected the annual penetration test results to determine that penetration tests were performed at least annually, using a methodology / frequency which aligned with compliance requirements and customer commitments.	No exceptions noted.
		Inquired of management and inspected the penetration test report to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether 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.	Not tested. No corrective actions were required during the period.
	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 organization 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 vulnerability scanning frequency configurations, a sample of monthly scans, and scan results to determine that scans were performed at least monthly in compliance with established security protocols for timely detection of system vulnerabilities.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected tickets for a sample of critical and high security deficiencies to determine that remediation plans were developed, implemented, and tracked within internal tools until resolution during vulnerability detection activities.	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 incident reporting settings on the intranet to determine that the organization provided internal personnel (employees & extended workforce) with instructions and mechanisms for reporting potential security & privacy concerns or incidents to the responsible team(s).	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 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 organization maintained internal policies and procedures regarding the notification of data breaches and investigative inquiries, in accordance with applicable laws.	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 organization had established an incident response policy that was reviewed annually and outlined management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents, which were categorized by severity.	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 incident reporting settings on the intranet to determine that the organization provided internal personnel (employees & extended workforce) with instructions and mechanisms for reporting potential security & privacy concerns or incidents to the responsible team(s).	No exceptions noted.
	The organization maintains a framework that defines how to organize a response to security & privacy incidents.	Inspected internal incident response webpages and Security Incident Response Team processes within the Information Security and Privacy Incident Response Policy to determine that a framework was in place for organizing a response to security and privacy incidents.	No exceptions noted.
	Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inspected the Information Security and Privacy Incident Response Policy to determine that information security incidents were required to be documented per the organization's Incident Response Policy.	No exceptions noted.
		Inspected the root cause analysis and remediation documentation for a sample of security event and incident tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents were used to strengthen and improve security controls, prevent future incidents, and could be used as examples for information security training.	No exceptions noted.
		Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated for potential impact on security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected a sample of security incident tickets to determine that security incidents were logged, tracked, resolved, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	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 Disaster Resiliency (DR) and Business Continuity (BC) planning documentation and testing checklists to determine that DR and BC testing was required to be conducted at least annually and included communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.
		Inspected DR and BC testing documentation and results to determine that the organization 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 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 organization had established an incident response policy that was reviewed annually and outlined management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents, which were categorized by severity.	No exceptions noted.

System Operations			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Information security incidents are documented per the organization's Incident Response Policy. Information from these events are used to strengthen and improve security controls, prevent future incidents, and can be used as examples for information security training.	Inspected the Information Security and Privacy Incident Response Policy to determine that information security incidents were required to be documented per the organization's Incident Response Policy.	No exceptions noted.
		Inspected the root cause analysis and remediation documentation for a sample of security event and incident tickets to determine that information security incidents were documented per the organization's Incident Response Policy and that information from these security incidents were used to strengthen and improve security controls, prevent future incidents, and could be used as examples for information security training.	No exceptions noted.
		Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated for potential impact on security commitments and objectives, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.
		Inspected a sample of security incident tickets to determine that security incidents were logged, tracked, resolved, and communicated to affected parties by management according to the organization's security incident response policies and procedures.	No exceptions noted.
	The organization maintains a framework that defines how to organize a response to security & privacy incidents.	Inspected internal incident response webpages and Security Incident Response Team processes within the Information Security and Privacy Incident Response Policy to determine that a framework was in place for organizing a response to security and 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 organization's systems were tested prior to deployment.	No exceptions noted.
	Changes to network configurations are reviewed and approved prior to deployment.	Inspected the documented change request tickets for a sample of network configuration changes to determine that changes to network configurations were reviewed and approved prior to deployment.	No exceptions noted.
	A standard image is utilized for the installation and maintenance of each production server.	Inspected the Change Management Policy, the organization's Source Code Guidelines, and the GDC connected Software Development Lifecycle (SDLC) document to determine that a standard image was required to be utilized for the installation and maintenance of each production server.	No exceptions noted.
		Inspected the configurations of example standard images deployed to production to determine that standard images were utilized for the installation and maintenance of production servers.	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 required to be 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.
	The organization has established guidelines for governing the installation of software on organization-owned assets.	Inspected the Third-Party Software Installation Security Guidelines to determine that guidelines were established to govern software installation on organization-owned assets.	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 system, rollback procedures, Change Management Security Policy, and CDPA to determine that a version control system was in place to manage source code, documentation, release labeling, and other functions and that safeguards were provided to ensure the integrity and availability of cloud customer data during system restorations.	No exceptions noted.

Change Management			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		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 organization used the version control system to manage source code, documentation, release labeling, and other functions.	No exceptions noted.
		Inspected evidence from the annual critical access group membership review, including a sample of users with access to the version control system and their respective job titles, to determine that access was reviewed and approved through the annual review process.	No exceptions noted.
	The organization has policies and guidelines governing the secure development lifecycle.	Inspected the Security Design in Applications, Systems, and Guidelines, and the Security Requirements for Outsourced Software Development Policy to determine that the organization had established policies and guidelines governing the secure development lifecycle, including outsourced development.	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 network configurations to determine that the implementation of information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
		Inspected the CDPA to determine that the organization communicated customer responsibilities to support service redundancy and availability of customer data through the implementation of backups within the organization's information processing resources.	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 organization 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 management of the organization 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 organization had established an incident response policy that was reviewed annually and outlined management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents, which were categorized by severity.	No exceptions noted.

Risk Mitigation			
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 incident reporting settings on the intranet to determine that the organization provided internal personnel (employees & extended workforce) with instructions and mechanisms for reporting potential security & privacy concerns or incidents to the responsible team(s).	No exceptions noted.
	The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected Disaster Resiliency (DR) and Business Continuity (BC) planning documentation and testing checklists to determine that DR and BC testing was required to be conducted at least annually and included communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.
		Inspected DR and BC testing documentation and results to determine that the organization 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 Privacy, Safety Security Org (PSS) 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. A portion of the control did not operate during the period because the circumstances that warrant the	Inspected the Vendor Security Assessment Guidelines to determine that the PSS Org had a documented, risk-based approach to reviewing the security practices of vendors and the security posture of vendor products.	No exceptions noted.
		Inquired of management and inspected the population of third-party vendors and subprocessors to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether both	Not tested. There were no applicable external parties employed by GDC

Risk Mitigation			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	operation of the control did not occur during the period. There were no applicable external parties employed by GDC connected during the period.	automated and manual assessments were performed based on data sensitivity.	connected during the period.
	The organization has policies and guidelines that govern third-party relationships.	Inspected the Google VSA Guidelines and support tool dashboards to determine that policies and procedures were developed to govern third-party relationships.	No exceptions noted.
	The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Inspected the nondisclosure agreement (NDA) templates to determine that the organization's agreements, including NDAs, provided details on preserving confidentiality of information and software exchanges.	No exceptions noted.
		Inspected the Google Cloud Platform ToS to determine that the organization established agreements 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 vendors/service providers and partners, respectively.	Inspected the CDPA template to determine that the organization required external parties (Service Providers) to meet security & privacy requirements for safeguarding user data and that requirements were enforced via the "Information Protection Addendum (IPA)" or the "Partner Information Protection Addendum (PIPA)" for vendors/service providers and partners, respectively.	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 in-scope systems to determine that the organization had implemented a contractual addendum 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 organization'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 organization's resource management documentation to determine that procedures related to managing information processing resources were made available and included guidance on requesting, monitoring, and maintaining resources, as well as forecasting capacity requirements to identify usage trends and manage system overload.	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 and Device Configuration Guidelines to determine that monitoring tools were documented to send automated alerts to operational personnel based on predetermined criteria, with incidents escalated per policy.	No exceptions noted.
		Inspected alert configurations and an example alert sent from monitoring tools to operational personnel to determine that automated alerts were sent based on predetermined criteria, with incidents 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 Security Logging Policy, Vulnerability Management Guidelines, Vulnerability Severity Guidelines, and alerting configurations to determine that policies and protection mechanisms were documented and configured for detecting and reporting operational issues.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
		Inspected monitoring tool dashboards, alerting configurations, and an example alert to determine that monitoring tools were provided to personnel for detecting and reporting operational issues.	No exceptions noted.
	The organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting based on usage and system performance.	Inspected the resource management policies and procedures to determine that the capacity of the organization's information processing resources was managed through a combination of planning, monitoring, and adjusting based on usage and system performance.	No exceptions noted.
		Inspected the internal capacity monitoring dashboards to determine that the organization managed the capacity of its information processing resources through a combination of planning, monitoring, and adjusting based on usage and system performance.	No exceptions noted.
		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.		
	Backups are periodically performed to support the availability of customer data.	Inspected internal backup and restoration instructional guidelines to determine that backups were required to be performed 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.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	Restore tests are periodically performed to confirm the ability to recover user data.	Inspected the disaster recovery testing post-mortem to determine that backup restoration testing was performed during the period to support the ability to recover user data.	No exceptions noted.
	The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected Disaster Resiliency (DR) and Business Continuity (BC) planning documentation and testing checklists to determine that DR and BC testing was required to be conducted at least annually and included communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.
		Inspected DR and BC testing documentation and results to determine that the organization 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 network configurations to determine that the implementation of information processing resources were distributed across distinct, geographically dispersed processing facilities to support service redundancy and availability.	No exceptions noted.
		Inspected the CDPA to determine that the organization communicated customer responsibilities to support service redundancy and availability of customer data through the implementation of backups within the organization's information processing resources.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The organization manages the capacity of its information processing resources through a combination of planning, monitoring and adjusting based on usage and system performance.	Inspected the resource management policies and procedures to determine that the capacity of the organization's information processing resources was managed through a combination of planning, monitoring, and adjusting based on usage and system performance.	No exceptions noted.
		Inspected the internal capacity monitoring dashboards to determine that the organization managed the capacity of its information processing resources through a combination of planning, monitoring, and adjusting based on usage and system performance.	No exceptions noted.
		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.
A1.3	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 Business Impact Analysis (BIA), DR test plan, and recovery playbooks to determine that requirements were established for BC 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 BIA and GDCE operational documentation to determine that the organization had implemented BC measures to maintain the availability of the organization's production infrastructure and services.	No exceptions noted.

Availability			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).	Inspected Disaster Resiliency (DR) and Business Continuity (BC) planning documentation and testing checklists to determine that DR and BC testing was required to be conducted at least annually and included communication plans, failover scenarios, operational transitions, and other emergency responses.	No exceptions noted.
		Inspected DR and BC testing documentation and results to determine that the organization 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 periodically performed to support the availability of customer data.	Inspected internal backup and restoration instructional guidelines to determine that backups were required to be performed 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.
	Restore tests are periodically performed to confirm the ability to recover user data.	Inspected the disaster recovery testing post-mortem to determine that backup restoration testing was performed during the period to support the ability to recover user 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.		
	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 configurations enforcing required approvals 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.
	The organization has policies and guidelines in place which govern the use and protection of identifiable data.	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 and that guidelines were in place which governed the use and protection of identifiable data.	No exceptions noted.
		Inspected 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.

Confidentiality			
TSC Reference	**Trust Services Criteria and Applicable Control Activities**	**Service Auditor's Tests**	**Results of Tests**
	The organization has established policies and guidelines to govern data classification, labeling and security.	Inspected the GDCE Service Terms, the CDPA, and the DPST to determine that the Company established policies and guidelines to define customer data and govern data classification, labeling, and security.	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. A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No data deletions occurred during the period.	Inspected the Data Destruction Guidelines and User Data Wipeout Policy to determine that the organization had procedures in place to dispose of confidential and ntk information in accordance with the data retention and deletion policy.	No exceptions noted.
		Inquired of management and inspected data deletion documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether the organization implemented procedures to dispose of confidential information according to the data retention and deletion policy.	Not tested. No data deletions occurred during the period.
	The organization establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchanges with external parties.	Inspected the nondisclosure agreement (NDA) templates to determine that the organization's agreements, including NDAs, provided details on preserving confidentiality of information and software exchanges.	No exceptions noted.
		Inspected the Google Cloud Platform ToS to determine that the organization established agreements 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. A portion of the control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No data deletions occurred during the period.	Inspected the Data Destruction Guidelines and User Data Wipeout Policy to determine that the organization had procedures in place to dispose of confidential and ntk information in accordance with the data retention and deletion policy.	No exceptions noted.
		Inquired of management and inspected data deletion documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether the organization implemented procedures to dispose of confidential information according to the data retention and deletion policy.	Not tested. No data deletions occurred during the period.
	The organization maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers.	Inspected the organization's CDPA, the Data Processing and Security Terms (DPST), and the GDC connected Service Terms on the publicly available Company website to determine that the organization 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 policies and guidelines to determine that the organization was required to sanitize storage media prior to disposal, release from organizational control, or release for reuse.	No exceptions noted.