

JOHANSON GROUP

System and Organization Controls (SOC) 3

Relevant to the Trust Services Criteria for
Security, Availability, and Confidentiality

For the Period
January 15, 2025 to January 14, 2026

Together with Independent Service
Auditor's Report

Gigs

TABLE OF CONTENTS

I.	Independent Service Auditor's Report	3
II.	Assertion of Gigs, Inc. Management	6
III.	Description of the Gigs Platform	8





Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

Gigs, Inc.

Scope

We have examined Gigs, Inc.'s accompanying assertion titled "Assertion of Gigs, Inc. Management" (assertion) that the controls within Gigs, Inc.'s Gigs Platform (system) were effective throughout the period January 15, 2025 to January 14, 2026, to provide reasonable assurance that Gigs, Inc.'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 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

Service Organization's Responsibilities

Gigs, Inc. 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 Gigs, Inc.'s service commitments and system requirements were achieved. Gigs, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Gigs, Inc. is responsible for selecting and identifying in its assertion the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective in achieving Gigs, Inc.'s service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective in achieving Gigs, Inc.'s service commitments and system requirements based on the applicable trust services criteria.

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

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

Inherent Limitations

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

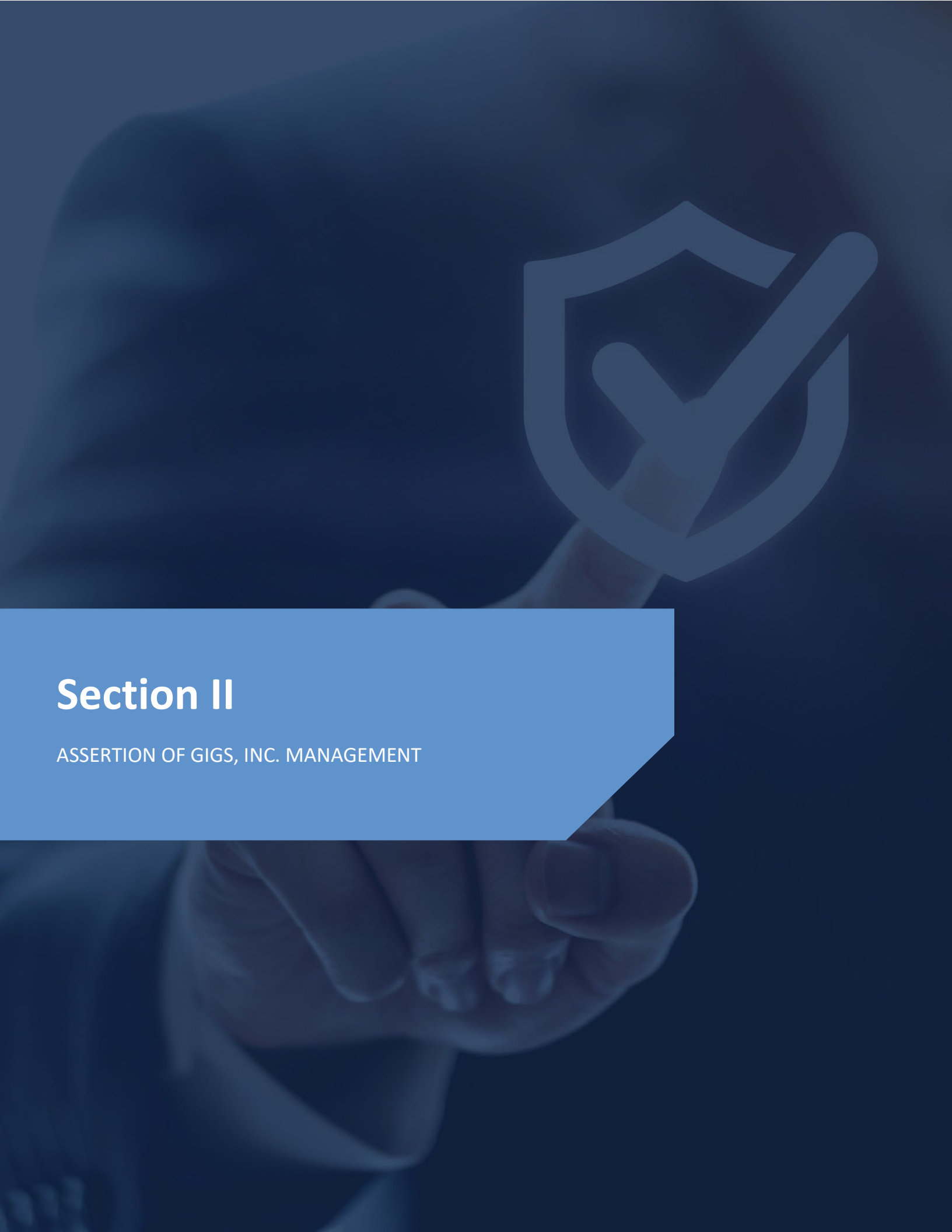
Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the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

Opinion

In our opinion, management's assertion that the controls within Gigs, Inc.'s Gigs Platform were effective throughout the period January 15, 2025 to January 14, 2026, to provide reasonable assurance that Gigs, Inc. service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

JohansonGroup LLP

Colorado Springs, Colorado
March 11, 2026



Section II

ASSERTION OF GIGS, INC. MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Gigs, Inc.'s Gigs Platform (system) throughout the period January 15, 2025 to January 14, 2026, to provide reasonable assurance that Gigs, Inc.'s service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of Gigs Platform" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 15, 2025 to January 14, 2026, to provide reasonable assurance that Gigs, Inc.'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 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

Gigs, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

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

We assert that the controls within the system were effective throughout the period January 15, 2025 to January 14, 2026, to provide reasonable assurance that Gigs, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Gigs, Inc. Management
March 11, 2026



Section III

DESCRIPTION OF THE GIGS PLATFORM

COMPANY BACKGROUND

Gigs, Inc. (“Gigs”) enables any company to sell mobile phone subscriptions (including data, text, and voice) to its customers.

Gigs, Inc. was incorporated in 2021 in the USA, and has wholly-owned subsidiaries in the USA (Gigs Wireless, LLC), the United Kingdom (Gigs U.K. Ltd), Germany (Gigs GmbH), France (Gigs FR SAS), Ireland (Gigs Wireless IE), and Brazil (GIGS BR LTDA).

DESCRIPTION OF SERVICES OVERVIEW OR SERVICES PROVIDED

The Gigs Platform provides API and SaaS solutions enabling companies to integrate and manage the mobile phone subscription lifecycle within their own products. The system description in this section of the report details only the Gigs Platform. Any other Gigs services are not within the scope of this report.

The Gigs Platform includes:

- **Gigs API:** A set of APIs enabling companies to deploy end-user activation, subscription management, billing, and SIM management.
- **Gigs Connect:** A white-label SaaS solution for checkout and subscription management. End users can sign up, pay, activate their SIM, and manage their subscription.
- **Gigs Dashboard:** An administrative SaaS for companies to manage subscriptions and see payment, device, and analytics data, as well as download reports.
- **Gigs Payments:** Multi-currency payments suite integrated into Gigs API and Gigs Connect. Includes recurring and one-time transactions as well as global tax handling.
- **Gigs for Work:** Providing fully automated employee phone plans for global teams.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Gigs designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Gigs makes to user entities, the laws and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Gigs has established for the services. The system services are subject to the Security, Confidentiality, and Availability commitments established internally for its services.

Gigs' commitments to customers are communicated through Service Level Agreements (SLA) and/or Partner Agreements (PA), and to end users through the Terms of Service and Privacy Policy.

Security Commitments

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

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect end-user data both at rest and in transit.
- Use of data retention and data disposal.
- Uptime availability of production systems.
- Regular vulnerability scans over the systems, and penetration tests over the production environment.

Confidentiality commitments

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties.
- Confidential information must be used only for the purposes explicitly stated in agreements between Gigs and user entities.

Availability commitments

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer and end-user requests in a reasonably timely manner.
- Operational procedures supporting the achievement of availability commitments to user entities.
- Business continuity and disaster recovery plans focusing on service resilience and backup and restore procedures.

Components of the System

The System description is comprised of the following components:

- **Software:** The application programs and IT system software that support application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house
- **People:** The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- **Data:** The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- **Procedures:** The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

The Gigs Platform is hosted on Google Cloud (GCP). Google Cloud is contracted through service agreements to be responsible for environmental and physical controls. Gigs has configured its Google Cloud environment to meet the security, availability, and confidentiality requirements.

The infrastructure includes, but is not limited to, the components in the table below:

Component	Business Function	Hosted Location
Virtual machines	Data processing	Google Cloud
Databases	Customer data storage	Google Cloud
Firewalls	Network protection	Google Cloud
Computers	Productivity	n/a

Software

Software includes the programs and software that support the Gigs Platform. The list of software used to build, support, maintain, and monitor the Gigs Platform includes, but is not limited to, the components in the table below:

Component	Description
Operating Systems	Linux Operating Systems are used.
Data stores	Persistent customer and end user data reside in relational databases, non-relational document databases, and cloud storage instances.
Network infrastructure	Virtual Private Cloud services are used.
Application and infrastructure monitoring	The covered services are monitored using: • Google Cloud provided metrics • A SaaS application and systems monitoring and alarming solution • A real-time operational and business intelligence platform
Security	Security of covered services is managed using: • Security information and event tool • An automated configuration management tool • A security and compliance management tool

People

Gigs employs dedicated team members to handle major product functions, including operations and support. Gigs focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep Gigs and its data secure.

Gigs has a staff of approximately 100, organized in the following functional areas:

- **Executive Management:** Responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment. This includes, but is not limited to, the President, CEO, Chief of Staff, Chief Architect, Head of Product, Head of Engineering, and Head of Finance.
- **Engineering:** Responsible for the development, testing, deployment, and maintenance of changes; monitoring; incident response; data backup and recovery; and overall security.
- **Security and Compliance:** Responsible for design, development, implementation, operation, maintenance, and monitoring of information security controls for infrastructure and IT processes; incident response; and compliance with frameworks like SOC 2.
- **IT:** Responsible for access management and managing internal corporate systems, laptops, software, and other technology involved in employee productivity and business operations.
- **Legal:** Responsible for facilitating compliance across various regulatory bodies and contractual requirements.
- **People Team:** Responsible for facilitating day-to-day activities relating to personnel, including onboarding and offboarding relevant personnel to the corporate environment, workplace health, discipline, and performance evaluations.

Data

Data, as defined by Gigs, constitutes the following:

Gigs stores user and account data, including Personally Identifiable Information (PII) and other data from employees, candidates, customers, prospects, and end users. This collection is permitted under the Terms of Service and Privacy Policies, as well as other separate agreements. Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized into the following major types of data used by Gigs.

Category	Description	Examples
Confidential	Access to confidential information is restricted to specific roles only.	• Personally Identifiable Information • Company banking and financial data • Production authentication credentials • Production secrets, private keys, and certificates
Internal	Access to internal information is protected from external access.	• Non-production secrets, private keys, and certificates • Internal policies and procedures • Internal documentation and RFCs • Meeting minutes and internal presentations
Public	Public information may have external access without any implications for Gigs.	• News and public announcements • Marketing materials, websites, and social media • Product documentation • External-facing policies

End user data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in end user agreements, if any. End-user data is captured, which is utilized by Gigs in delivering its services.

All employees and contractors of Gigs are obligated to respect and, in all cases, to protect end-user data. Additionally, Gigs has policies and procedures in place for proper and secure handling of end-user data. These policies and procedures are reviewed at least on an annual basis.

PROCESSES AND PROCEDURES

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners.

The following procedures cover the relevant operations of the Gigs Platform:

- Access Management
- Backup Management
- Business Continuity and Disaster Recovery
- Change Management
- Configuration Management

- Data Management
- Incident Management
- Mobile Device Management
- Network Operations
- Risk Assessment
- Security Training
- Vendor Management
- Vulnerability Management

Physical Security

Gigs' production environment, including servers and networks, is maintained by Google Cloud. The physical and environmental security protections are the responsibility of Google Cloud. Gigs reviews the attestation reports and performs a risk analysis of Google Cloud on at least an annual basis.

Logical Access

Gigs provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and consistent user provisioning and de-provisioning processes.

Access to systems is split into at least admin roles, user roles, and no access. User access and roles on high-risk systems are reviewed at least every six months to ensure least privilege access.

The IT team is responsible for providing access to the system based on the employee's role. Employees are responsible for reviewing Gigs' policies and completing security training.

When an employee is terminated, the IT team is responsible for de-provisioning access to all in-scope systems within 24 hours to high-risk systems and within 5 business days to lower-risk systems.

Computer Operations - Backups

End-user data is backed up and monitored by the Engineering team for completion and exceptions. If there is an exception, the Engineering team will perform troubleshooting to identify the root cause and either rerun the backup or let it run as part of the next scheduled backup job.

Backup infrastructure is maintained in Google Cloud with physical access restricted according to the policies. Backups are encrypted, and access is restricted to relevant personnel.

Computer Operations - Availability

Gigs maintains an incident response plan to guide employees on reporting and responding to any availability, information security, or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

Gigs internally monitors all applications, including the web UI, databases, and cloud storage, to ensure that service delivery matches SLA requirements.

Vulnerabilities

Gigs uses the following means to detect vulnerabilities:

- Third-party dependency scanning on GitHub (continuously)
- Infrastructure vulnerability scanning on Google Cloud (continuously)
- Penetration tests conducted by a third party (at least annually)

Identified vulnerabilities are tracked and responded to in accordance with internal SLAs.

Change Management

Gigs maintains documented Secure Software Development policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, and required approval procedures.

A system is utilized to document the change control procedures for changes in the application and implementation of new changes. Testing results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Changes are approved prior to migration to the production environment, and approvals are documented.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Gigs uses Google Cloud to run its production infrastructure, which assures network monitoring, configuration, and operations. Google Cloud simplifies the logical network configuration by providing an effective firewall around all of Gigs' application containers, with the only ingress allowed coming via designated public-facing endpoints.

Google Cloud also automates the provisioning and de-provisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on the underlying hardware.

BOUNDARIES OF THE SYSTEM

The boundaries of the Gigs Platform are the specific aspects of the Gigs' infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers and end users. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Gigs Platform.

This report does not include the Cloud Hosting Services provided by Google Cloud at multiple facilities.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

Common Criteria (to the Security, Availability, and Confidentiality Categories)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage, and ii. systems that use electronic information to process, transmit, or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removals of information or system resources, misuse of the software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations, or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary and intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding the collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Gigs' control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Gigs' ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management’s actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Employees are required to sign an acknowledgment form indicating they have been given access to and understand their responsibility for adhering to Gigs' policies.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties, is a component of employee and contractor contracts.
- Background reference checks are performed in accordance with local laws and regulations, and completed prior to or at the latest 30 days after the start date.

Commitment to Competence

Gigs' management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated the required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

The Gigs management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers and end users entrust to us.

The management team is frequently briefed on technology changes that impact the way Gigs can help customers build products, as well as new security technologies that can help protect these products, and finally, any regulatory changes that may require Gigs to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with the core product offerings and duties to new and existing customers and end users.

Specific control activities that the service organization has implemented in this area are described below:

- Management is briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

Gigs' organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Gigs' assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate

business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Gigs' success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensure the service organization is operating at maximum efficiency. Gigs' human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for Gigs' policies and a confidentiality agreement.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

RISK ASSESSMENT PROCESS

Gigs' risk assessment process identifies and manages risks that could potentially affect Gigs' ability to provide reliable and secure services to customers and end users. As part of this process, Gigs maintains a risk register to track systems and procedures that could present risks to meeting Gigs' objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Gigs product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates, the commitments, agreements, and responsibilities of Gigs' system, as well as the nature of the components of the system, result in risks that the criteria will not be met. Gigs addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Gigs' management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

INFORMATION AND COMMUNICATION SYSTEMS

Information and communication are an integral component of Gigs' internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Gigs uses several information and communication channels internally to share information with management, employees, contractors, and customers. Gigs uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Gigs uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Gigs' management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from Gigs' policies and procedures. Employee activity and adherence to Gigs' policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Gigs' management conducts quality assurance monitoring on a regular basis, and additional training is provided based on the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Gigs' operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in Gigs' procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Gigs' personnel.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in Gigs' policies. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within internal tracking tools. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

CHANGES TO THE SYSTEM

No significant changes have occurred to the services provided during the review period.

INCIDENTS

No security incidents

CRITERIA NOT APPLICABLE TO THE SYSTEM

The trust service criteria, Privacy and Processing Integrity, were not tested during this audit; they were not applicable.

SUBSERVICE ORGANIZATIONS

This report does not include the Cloud Hosting Services provided by Google Cloud at multiple facilities.

SUBSERVICE DESCRIPTION OF SERVICES

The Cloud Hosting Services provided by Google Cloud support the physical infrastructure of the entity's services.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

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

The following subservice organization controls have been implemented by Google Cloud and included in this report to provide additional assurance that the trust services criteria are met.

Subservice Organization - Google Cloud (GCP)		
Category	**Criteria**	**Control**
Security	CC 6.4	Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge access readers, biometric identification mechanisms, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high-security areas in data centers are reviewed on a defined basis, and inappropriate access is removed in a timely manner.
		Visitors to center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually, and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel using real-time video surveillance and/or alerts generated by security systems.
Availability	A 1.2	Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.
		Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).
		Data centers are equipped with fire detection alarms and protection equipment.
		The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy and availability.
		The organization conducts disaster resiliency testing (DiRT), which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).

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

- Reviewing and reconciling output reports.
- Holding periodic discussions with vendors and subservice organization(s).
- Testing controls performed by vendors and subservice organization(s).
- Reviewing attestation reports over services provided by vendors and subservice organization(s).
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations.

COMPLEMENTARY USER ENTITY CONTROLS

Gigs' services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Gigs' services to be solely achieved by Gigs control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Gigs.
The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Gigs.
2. User entities are responsible for notifying Gigs of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Gigs services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Gigs services.
6. User entities are responsible for providing Gigs with a list of approvers for security and system configuration changes for data transmission.
1. User entities are responsible for immediately notifying Gigs of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.