A-LIGN

A-LIGN.com

Type 2 SOC 2

Prepared for:
Glooko, Inc.

Year:
2026

glooko®
BETTER TOGETHER

REPORT ON GLOOKO, INC.'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY

Pursuant to Reporting on System and Organization Controls 2 (SOC 2)
Type 2 examination performed under AT-C 105 and AT-C 205

June 1, 2026 to August 31, 2026

Table of Contents

SECTION 1 ASSERTION OF GLOOKO, INC. MANAGEMENT 1

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT 3

SECTION 3 GLOOKO, INC.'S DESCRIPTION OF ITS ENDOTOOL IV GLUCOSE MANAGEMENT SYSTEM CLOUD THROUGHOUT THE PERIOD JUNE 1, 2026 TO AUGUST 31, 2026 7

OVERVIEW OF OPERATIONS 8
Company Background 8
Description of Services Provided 8
Principal Service Commitments and System Requirements 8
Components of the System 9
Boundaries of the System 13
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING 14
Control Environment 14
Risk Assessment Process 15
Information and Communications Systems 16
Monitoring Controls 16
Changes to the System in the Last 3 Months 17
Incidents in the Last 3 Months 17
Criteria Not Applicable to the System 17
Subservice Organizations 17
COMPLEMENTARY USER ENTITY CONTROLS 18
TRUST SERVICES CATEGORIES 19

SECTION 4 TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS 20

GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS 21
CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION 22
TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY 22

SECTION 5 OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION 130

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS 131

SECTION 1

ASSERTION OF GLOOKO, INC. MANAGEMENT

ASSERTION OF GLOOKO, INC. MANAGEMENT

September 7, 2026

We have prepared the accompanying description of Glooko, Inc.'s ('Glooko' or 'the Company') EndoTool IV Glucose Management System Cloud titled "Glooko, Inc.'s Description of Its EndoTool IV Glucose Management System Cloud throughout the period June 1, 2026 to August 31, 2026" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the EndoTool IV Glucose Management System Cloud that may be useful when assessing the risks arising from interactions with Glooko's system, particularly information about system controls that Glooko 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 (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

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

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

a. the description presents Glooko's EndoTool IV Glucose Management System Cloud that was designed and implemented throughout the period June 1, 2026 to August 31, 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period June 1, 2026 to August 31, 2026, to provide reasonable assurance that Glooko's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Glooko's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period June 1, 2026 to August 31, 2026, to provide reasonable assurance that Glooko's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Glooko's controls operated effectively throughout that period.

Benjamin Chang

Benjamin Chang
VP, Security and IT Operations
Glooko, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Glooko, Inc.

Scope

We have examined Glooko's accompanying description of its EndoTool IV Glucose Management System Cloud titled "Glooko, Inc.'s Description of Its EndoTool IV Glucose Management System Cloud throughout the period June 1, 2026 to August 31, 2026" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 1, 2026 to August 31, 2026, to provide reasonable assurance that Glooko's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Glooko uses AWS to provide cloud hosting services for its Cloud solution. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Glooko, to achieve Glooko's service commitments and system requirements based on the applicable trust services criteria. The description presents Glooko's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Glooko'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.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Glooko, to achieve Glooko's service commitments and system requirements based on the applicable trust services criteria. The description presents Glooko's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Glooko's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The information included in Section 5, "Other Information Provided by the Service Organization," is presented by Glooko management to provide additional information and is not a part of the description. Information about Glooko's management's response to testing exceptions has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Glooko's service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

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

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

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

Independence and Ethical Responsibilities

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

Inherent Limitations

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

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

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

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects,

a. the description presents Glooko's EndoTool IV Glucose Management System Cloud that was designed and implemented throughout the period June 1, 2026 to August 31, 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period June 1, 2026 to August 31, 2026, to provide reasonable assurance that Glooko's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Glooko's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period June 1, 2026 to August 31, 2026, to provide reasonable assurance that Glooko's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Glooko'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 Glooko, user entities of Glooko's EndoTool IV Glucose Management System Cloud during some or all of the period June 1, 2026 to August 31, 2026, business partners of Glooko subject to risks arising from interactions with the EndoTool IV Glucose Management System Cloud, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

A-LIGN ASSURANCE

Tampa, Florida
September 7, 2026

SECTION 3

GLOOKO, INC.'S DESCRIPTION OF ITS ENDOTOOL IV GLUCOSE MANAGEMENT SYSTEM CLOUD THROUGHOUT THE PERIOD JUNE 1, 2026 TO AUGUST 31, 2026

OVERVIEW OF OPERATIONS

Company Background

Monarch Medical Technologies ('Monarch') was founded in 2012 with the objective of providing patient-specific insulin dosing software in the United States (US). Monarch has designed and implemented a solution to streamline nursing workflows while prioritizing patient safety. In 2025, Monarch was acquired by Glooko, Inc. to expand Glooko's connected care capabilities into inpatient glycemic management.

Description of Services Provided

With the Monarch acquisition, Glooko provides cloud-hosted patient-specific insulin dosing software services throughout the United States. The EndoTool IV Glucose Management System Cloud is a multiuser, transaction-based application suite that enables the processing and delivery of insulin dosing guidance. EndoTool enables processing of the following tasks:

- Capturing clinical data for healthcare providers and facilities
- Determining patient-specific insulin dosing requirements
- Providing clinical decision support for insulin management
- Managing user access and ensuring compliance with healthcare regulations
- Providing operational and management reporting

Information is shared with user entities using secured cloud-based access via Hyper Text Transfer Protocol Secure/ Transport Layer Security (HTTPS/TLS) protocols.

Glooko establishes operational requirements that support the achievement of security commitments, service levels, relevant laws and regulations, and other system requirements. Such requirements are communicated in Glooko's system policies and procedures, system design documentation, and contracts and Service Level Agreements (SLA)s with customers, vendors and third-parties. Changes to commitments, requirements, and responsibilities are communicated to external parties, including impacted customers and vendors.

Organizational and information security policies are formally documented to support the functioning of internal controls and processes and define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the EndoTool IV Cloud Software. Glooko ensures that the company's organizational and information security policies and procedures are made available to its personnel.

Principal Service Commitments and System Requirements

Glooko designs its processes and procedures related to EndoTool IV Glucose Management System Cloud to meet its objectives for its cloud hosted software solutions. Those objectives are based on the service commitments that Glooko makes to user entities, the laws and regulations that govern the provision of its cloud hosted software solutions, and the financial, operational, and compliance requirements that Glooko has established for the services.

Glooko's cloud-hosted software solutions are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Glooko operates.

Security commitments to user entities are documented and communicated in the EndoTool IV Glucose Management System Cloud Cyber Security Labeling, SLAs and other customer agreements. Commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the EndoTool IV Glucose Management System Cloud that are designed to permit system users to access the information based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit is implemented. The encryption technologies and methods utilized are defined in the Encryption Policies and Procedures document. Critical data including personal information and passwords is required to be stored in an encrypted format. In addition, when employees utilize mobile devices to access in-scope systems, the connection must be established in a secure manner using encryption.

Glooko has established operational requirements that support the achievement of security commitments, service levels, compliance with relevant laws and regulations, and other system requirements. Such requirements are communicated in Glooko's system policies and procedures, system design documentation, and contracts and SLAs with customers, vendors and third-parties. Changes to commitments, requirements, and responsibilities are communicated to external parties, including impacted customers and vendors.

Organizational and information security policies are formally documented to support the functioning of internal controls and processes and define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the EndoTool IV Glucose Management System Cloud.

Glooko ensures that the company's organizational and information security policies and procedures are made available to its personnel.

Components of the System

Infrastructure

Primary infrastructure used to provide Glooko's EndoTool IV Glucose Management System Cloud includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Database Servers	Postgres	Database structure
Authentication	Amazon Web Services (AWS)	Identity and Access Management (IAM)
Authentication	Auth0	IAM
Networking	AWS Virtual Private Cloud (VPC)	Segments client networks and controls traffic
Storage	AWS Simple Storage Service (S3)	Storage of application data and backups

Software

Primary software used to provide Glooko's EndoTool IV Glucose Management System Cloud includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
EndoTool IV Cloud Software	Cloud-based	Clinical Decision Support
AWS (Amazon Web Services)	Cloud	Infrastructure Hosting
Jira	Cloud	Ticketing System
GitHub	Cloud	Software Version Control
PurpleBox	Software-as-a-Service (SaaS)	Penetration Testing
Aikido	SaaS	Vulnerability Scanning

People

Glooko has a staff of employees organized in the following functional areas:

- Corporate: Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, finance, human resources, and customer success management.
- Operations: Staff that administers the onboarding, configuration, and support of the EndoTool system for healthcare facilities. They provide direct services, including user administration, technical support, and clinical monitoring.
- Customer Support: Provides technical and clinical assistance to hospital users, facilitating the configuration and ongoing use of the EndoTool IV Glucose Management System Cloud.
- Clinical Services: Monitors system performance and provides clinical support, ensuring the software meets the therapeutic and safety needs of the healthcare facilities.
- Information Technology (IT) and Engineering: Help desk, IT infrastructure, system administration, software development, application support, and information security personnel manage cloud environments and business support systems.
- Engineering/DevOps: Develops and maintains the EndoTool IV Cloud software, supporting utilities, and the cloud hosting infrastructure in AWS.
- IT/Security: Supports the system indirectly by monitoring internal and external security threats, maintaining security controls, (firewall and IDS) and managing access.

Data

Data, as defined by Glooko, constitutes the following:

- Clinical transaction data
- User access and identity data
- Configuration and facility settings
- System audit logs
- Electronic interface/API exchange data
- Security and vulnerability scan logs

The audit log captures and records key activities and events, including the start and end of user sessions, web browser identification, and login attempts. It tracks specific actions such as patient enrollment steps, access to patient records, and entry of patient data.

Additionally, it logs critical processes like dose calculations, saving downtime reports, and the exit from patient records. Security-related events such as system errors, data validation failures, and the expiration of patient lockout times are also documented, providing a comprehensive record of user interactions and system responses.

Data classification policies and procedures are formally established to define the criticality of the data, data classification schemes, who can access what data, how data is secured, how long data should be retained, and how/when it is purged or destroyed. Data must be classified and structured in a consistent manner. As data is no longer required for business purposes, it is appropriately purged or destroyed. Where there is electronic Protected Health Information (ePHI) data on a device or media that is no longer required, the Company ensures to sanitize the ePHI data prior to the device or media being re-used. Appropriate internal controls have been implemented to protect confidential documents, files, or directories from inappropriate access. In addition, access to confidential and/or customer data is restricted to authorized personnel based on job role and responsibilities.

Management has defined and documented the components of the data critical to supporting the in-scope system including a description of what the critical data is and is used for, the source of the data, and how the data is stored and transmitted.

Operational personnel review data input, processed, and output from the in-scope system for completeness, accuracy, and timeliness. Errors in the processing of critical data are detected, investigated, and resolved in a timely manner.

As data is entered into the in-scope systems, edit checks are in place to help prevent incomplete or incorrect data from being entered in. In addition, the company has documented and maintains data flow diagrams, process flowcharts, narratives and procedures manuals to identify the relevant internal and external information sources of the system as well as how data moves within the environment.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Logical access includes system settings and configurations, password requirements, access management, authentication, and system and access logging requirements.

All teams are trained on and expected to adhere to the policies and procedures that define how services should be delivered. These are located on the company's document management system and can be accessed by any Glooko team member.

Physical Security

Glooko relies on AWS for cloud hosting services to support the in-scope infrastructure and systems for its Cloud solution. Refer to the "Subservice Organizations" section below for physical security controls implemented and operated by AWS.

Logical Access

Glooko employs Role-Based Access Control (RBAC). Access to SaaS based tools and the cloud environment is secured Single Sign-On (SSO) where available. Access rights and users for internal and production access are reviewed by management at least annually.

Access to server infrastructure is managed via AWS Identity and Access Management (IAM). Privileged access is restricted to authorized personnel based on job roles, and activity is logged and reviewed.

Computer Operations - Backups

Glooko utilizes AWS' platform-managed services for backups and data replication. Critical internal and customer data is backed up, encrypted, and replicated off-site to ensure high availability, resilience, and disaster recovery capability in alignment with System and Organization Controls (SOC) 2 requirements.

Computer Operations - Availability

Glooko leverages AWS' platform-managed infrastructure to ensure continuous availability, high resilience, and proactive capacity management.

Automated monitoring tools continuously evaluate system performance and resource utilization, generating alerts for potential issues to support rapid incident response and disaster recovery processes.

Change Control

Glooko maintains documented change management policies and procedures to guide personnel in documenting and implementing system (e.g. application, infrastructure, network, etc.) changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures. The change control procedures also outline the process to follow for emergency changes.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality Assurance (QA) testing and User Acceptance Testing (UAT) 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. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system. Access to promote changes to the production environment is restricted to authorized personnel requiring such access for their role and responsibilities.

Releases are approved by a Change Advisory Board and packed for distribution in a secure location. Changes promoted to the production environment are approved by customers prior to implementation.

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.

Glooko has implemented a patch management process to ensure EndoTool IV Glucose Management System Clouds are patched in accordance with recommended system patches. Changes made to in-scope systems are communicated to both internal and external users that are affected by the given change.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Antivirus endpoint protection software is installed on the in-scope production servers, which is configured to run scans and push updates regularly. The firewall systems and antivirus protection are configured according to the anti-malware and firewall policies and procedures.

An Intrusion Detection System (IDS) is in-place to prevent and detect unusual activity. The IDS system is configured to send alerts when potential threats or unusual system activity are detected. Alerts are investigated and resolved by support personnel. Administrative access to the firewall is restricted to authorized employees.

Glooko monitors the in-scope systems to identify potential security threats and vulnerabilities and to detect unusual system activity. The monitoring tools are configured to send alerts when potential threats or unusual system activity are detected. Alerts are investigated and resolved by support personnel.

The Company has formally defined policies and procedures in place regarding completing penetration tests and vulnerability scans and addressing and remediating identified vulnerabilities.

Penetration testing is conducted annually to measure the security posture of the target system. The third-party vendor uses an accepted industry standard penetration testing methodology. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed monthly and Penetration Testing at least annually in accordance with Glooko policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Glooko. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. To ensure robust security, Glooko conducts Aikido scans that leverage the Open Web Application Security Project (OWASP) and Network Vulnerability Scanning (NVS) databases to detect vulnerabilities. During the software development process, OWASP scans are performed at code freeze to identify and address any issues prior to software release. Scans are performed during non-peak windows.

Vulnerabilities identified from the penetration tests and vulnerability scans performed are formally documented, prioritized, addressed and remediated in a timely manner and in accordance with company policies and procedures.

Employees are authenticated through the use of a two-factor authentication system. User activity is configured to be logged via built-in monitoring tools, and those logs are retained and reviewed as needed. Privileged access to the cloud environment is restricted to authorized personnel requiring such access for their role and responsibilities.

Boundaries of the System

The scope of this report includes the EndoTool IV Glucose Management System Cloud performed in the remote facilities.

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

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

Integrity and ethical values are essential elements of Glooko's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Glooko's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. 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 include:

- Formally documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.
- Employees, third-parties, and customers are informed of how to report unethical behavior in a confidential manner.

Commitment to Competence

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

Specific control activities that the service organization has implemented in this area include:

- As part of the hiring process, management evaluates a candidate's competencies, skillsets, and prior experience.
- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Security awareness, HIPAA for Business Associates and Good Manufacturing Practices training is provided at least annually to maintain the knowledge of responsibilities of all personnel of critical processes.

Management's Philosophy and Operating Style

Glooko's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area include:

- 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 as a whole.

Organizational Structure and Assignment of Authority and Responsibility

Glooko's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes 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.

Glooko's 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. Job descriptions (including for Executive Management) are formally documented and communicated to employees, and management reviews the written job descriptions at least annually for accuracy.

Specific control activities that the service organization has implemented in this area include:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.
- Organizational charts are reviewed for accuracy at least annually by management.

Human Resources Policies and Practices

Glooko's 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 ensures the service organization is operating at maximum efficiency. Glooko's 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 include:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- 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

Glooko maintains a formal risk assessment process to identify, analyze, and manage risks that could impact the EndoTool IV Cloud platform's ability to provide reliable, secure services. This process aligns with the International Organization for Standardization (ISO) 14971:2019 risk management standard and is consistent with Glooko's enterprise risk methodology. Key components include an annual formal risk assessment covering fraud, vendors, third-parties, and changes to the environment (people, processes, technology). Vendor and third-party due diligence is performed to verify security posture, with identified control gaps addressed through formal remediation processes.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Glooko's EndoTool IV Glucose Management System Cloud; as well as the nature of the components of the system result in risks that the criteria will not be met. Glooko 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, Glooko's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication is an integral component of Glooko's 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. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Glooko, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, Meetings are held in each geographic location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead these meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Glooko personnel via e-mail messages.

Monitoring Controls

Glooko management monitors internal controls to ensure they operate as intended and adapt to changing operational conditions. Management continuously assesses the quality of internal controls over time using platforms like Drata to track control performance and compliance status. Necessary corrective actions are implemented to address any deviations from company policies and procedures, which are tracked via enterprise ticketing systems or the compliance platform. Employee activity and adherence to policies are monitored through ongoing activities and evaluations.

Glooko maintains a formal internal controls program detailing the implemented controls, roles and responsibilities, control frequency, types, and execution methods. Management conducts annual reviews to assess the effectiveness and performance of the internal control environment. Executive management maintains independence from those operating key internal controls to ensure objective oversight.

On-Going Monitoring

Glooko's management conducts regular quality assurance monitoring to ensure the effectiveness of internal controls. The organization utilizes Drata as its primary compliance monitoring platform to track ongoing control performance and ensure audit readiness for EndoTool IV Glucose Management System Cloud. Monitoring activities are utilized to initiate timely corrective actions through structured department meetings, internal technical syncs, and formal notifications. Furthermore, Glooko has assigned formal responsibility to dedicated compliance and security personnel for coordinating and monitoring all audit-related activities, ensuring that the internal control environment is evaluated at least annually.

Management maintains active oversight of operations to identify significant variances from expectations regarding internal controls. Upper management reviews facts and circumstances related to any potential control breakdown or identified risk. Decisions for addressing control weaknesses are made based on whether the incident is isolated or necessitates a change in company procedures, personnel, or infrastructure. The goal of this ongoing process is to ensure consistent legal compliance and to maximize the security and operational performance of the EndoTool IV Glucose Management System Cloud environment.

Reporting Deficiencies

Glooko utilizes Drata as its primary compliance and internal control tracking tool to document and monitor the results of on-going monitoring procedures and audit remediations for EndoTool IV Glucose Management System Cloud. System-related incidents and operational changes are tracked within an enterprise ticketing system. Escalation procedures are maintained for responding to and notifying management of any identified risks.

Risks receiving a high rating are prioritized for immediate response.

Corrective actions, when necessary, are documented and tracked within Jira. Management conducts recurring risk meetings to review reported deficiencies, the status of corrective actions, and the overall compliance posture.

Changes to the System in the Last 3 Months

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

Incidents in the Last 3 Months

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

Criteria Not Applicable to the System

All Common/Security criteria were applicable to Glooko, Inc.'s EndoTool IV Glucose Management System Cloud.

Subservice Organizations

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

Subservice Description of Services

Glooko relies on AWS for cloud hosting services to support the in-scope infrastructure and systems.

Complementary Subservice Organization Controls

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

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

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic IDS are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

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

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

COMPLEMENTARY USER ENTITY CONTROLS

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

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

1. User entities are responsible for understanding and complying with their contractual obligations to Glooko.
2. User entities are responsible for notifying Glooko 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 Glooko 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 Glooko, Inc.'s services.
6. User entities are responsible for providing Glooko with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Glooko of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

8. User entities are responsible for restricting access to system resources to appropriate user entity personnel.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security Category)
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 removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Control Activities Specified by the Service Organization

The applicable trust services criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Glooko, Inc.'s description of the system. Any applicable trust services criteria that are not addressed by control activities at Glooko, Inc.'s are described within Section 4 and within the "Subservice Organizations" section above.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

SECTION 4

TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

A-LIGN ASSURANCE's examination of the controls of Glooko was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Glooko and did not encompass all aspects of Glooko's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Determine whether the criteria are relevant to the user entity's assertions; and
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Personnel responsibilities for information security are communicated to and acknowledged by personnel.	Inquired of the VP, Security and IT Operations regarding the onboarding process to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
			Inspected the company policy acknowledgment for a sample of new hires to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
		Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	Inspected the code of conduct and completed performance and conduct evaluation form for a sample of current employees to determine that management conducted annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	No exceptions noted.
		Background checks are conducted on eligible personnel prior to hire as permitted by local laws.	Inquired of the VP, Security and IT Operations, regarding background checks to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the access control policies and procedures to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	No exceptions noted.
			Inspected the completed background check for a sample of new hires to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	Testing of the control activity disclosed that background check was not completed in a timely manner for one of one new hire sampled.
		The Company maintains a documented Code of Conduct. Eligible personnel are required to accept the Company's Code of Conduct during onboarding and annually thereafter.	Inspected the code of conduct and code of conduct acknowledgement for a sample of new hires and current employees to determine that the Company maintained a documented Code of Conduct, and eligible personnel were required to accept the Company's Code of Conduct during onboarding and annually thereafter.	No exceptions noted.
		The Company has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the Company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted.	Inquired of the VP, Information Security and IT regarding the disciplinary process to determine that the company had a defined disciplinary process to be enacted when a member of the workforce violated the company's policies or caused a security or privacy incident, and management retained documentation of instances when the disciplinary process was enacted.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the code of conduct to determine that the Company had a defined disciplinary sanctions process to be enacted when a member of the workforce violated the Company's policies or caused a security or privacy incident. Management retained documentation of instances when the disciplinary process was enacted.	No exceptions noted.
			Inspected the HR records to determine that the Company had a defined disciplinary sanctions process to be enacted when a member of the workforce violated the Company's policies or caused a security or privacy incident, and management retained documentation of instances when the disciplinary process was enacted.	Testing of the control activity disclosed that there were no instances where a member of the workforce violated the company's policies or caused a security or privacy incident during the review period.
		Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.	Inspected the company's website, compliance automation software, code of conduct, internal communication channel and incident management and escalation policies and procedures to determine that internal communication channels were in place for employees to report failures, events, incidents, concerns, and other issues to company management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The Company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the company's charter to determine that the Company's board of directors had a documented charter that outlined its oversight responsibilities for internal control.	No exceptions noted.
		The company's board of directors meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented.	Inspected the internal controls and operations review management meeting minutes to determine that the Company's board of directors met at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies, and meeting minutes, including decisions made and action items, were documented.	No exceptions noted.
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
		Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	Inspected the code of conduct and completed performance and conduct evaluation form for a sample of current employees to determine that management conducted annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The board of directors includes members independent from management who are not involved in control operations.	Inspected the board charter and board meeting minutes to determine that the board of directors included members independent from management who were not involved in control operations.	No exceptions noted.
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the information security policies and procedures, organizational chart, compliance automation software, and job description for a sample of job roles to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees and is updated upon changes to the organizational structure.	Inspected the organizational chart, including the revision history to determine that an organizational chart was in place to describe the organizational structure and reporting lines, and the chart was available to all employees and was updated upon changes to the organizational structure.	No exceptions noted.
		The Company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the company's charter to determine that the Company's board of directors had a documented charter that outlined its oversight responsibilities for internal control.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel responsibilities for information security are communicated to and acknowledged by personnel.	Inquired of the VP, Security and IT Operations regarding the onboarding process to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
			Inspected the company policy acknowledgment for a sample of new hires to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
		The board of directors includes members independent from management who are not involved in control operations.	Inspected the board charter and board meeting minutes to determine that the board of directors included members independent from management who were not involved in control operations.	No exceptions noted.
		The Company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role.	Inspected the job description for a sample of job roles to determine that the Company had documented job descriptions for each position at the company, which included roles and responsibilities as well as required qualifications, skills, and experience for the role.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company performs due diligence activities prior to engaging with a new service provider or vendor. Results of the due diligence activities including action items are documented.	Inspected the vendor listing and completed supplier evaluation form for a sample of third-parties to determine that the Company performed due diligence activities prior to engaging with a new service provider or vendor, and the results of the due diligence activities including action items were documented.	No exceptions noted.
		The Company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, are documented.	Inspected the compliance reports and associated security review documentation for a sample of third-parties to determine that the Company obtained and reviewed compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The Company has established training programs to help personnel gain awareness of information security best practices. Personnel are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary.	Inspected the information security policies and procedures and training completion certificates for a sample of new hires and current employees to determine that the Company had established training programs to help personnel gain awareness of information security best practices, personnel were required to complete the training during onboarding, and periodic refresher training is provided to personnel at least annually and as deemed necessary.	No exceptions noted.
		Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	Inspected the code of conduct and completed performance and conduct evaluation form for a sample of current employees to determine that management conducted annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	No exceptions noted.
		Background checks are conducted on eligible personnel prior to hire as permitted by local laws.	Inquired of the VP, Security and IT Operations, regarding background checks to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the access control policies and procedures to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	No exceptions noted.
			Inspected the completed background check for a sample of new hires to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	Testing of the control activity disclosed that background check was not completed in a timely manner for one of one new hire sampled.
		Management evaluates candidates for employment through a formal screening process. The process may include verification of academic and professional qualifications, identity verifications, validation of personal or professional references, technical interviews, or other steps as deemed applicable by the organization.	Inspected the interview meeting schedule for a sample of new hires to determine that management evaluated candidates for employment through a formal interview process. The process included verification of academic and professional qualifications, identity verifications, validation of personal or professional references, technical interviews, or other steps as deemed applicable by the organization.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company performs due diligence activities prior to engaging with a new service provider or vendor. Results of the due diligence activities including action items are documented.	Inspected the vendor listing and completed supplier evaluation form for a sample of third-parties to determine that the Company performed due diligence activities prior to engaging with a new service provider or vendor, and the results of the due diligence activities including action items were documented.	No exceptions noted.
		The Company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, are documented.	Inspected the compliance reports and associated security review documentation for a sample of third-parties to determine that the Company obtained and reviewed compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, were documented.	No exceptions noted.
		Policies and procedures are in place that outline the talent acquisition, performance evaluation and annual training processes.	Inspected the employee performance evaluation policies and procedures and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the talent acquisition, performance evaluation and annual training processes.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees and is updated upon changes to the organizational structure.	Inspected the organizational chart, including the revision history to determine that an organizational chart was in place to describe the organizational structure and reporting lines, and the chart was available to all employees and was updated upon changes to the organizational structure.	No exceptions noted.
		Personnel responsibilities for information security are communicated to and acknowledged by personnel.	Inquired of the VP, Security and IT Operations regarding the onboarding process to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
			Inspected the company policy acknowledgment for a sample of new hires to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
		Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	Inspected the code of conduct and completed performance and conduct evaluation form for a sample of current employees to determine that management conducted annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company maintains a documented Code of Conduct. Eligible personnel are required to accept the Company's Code of Conduct during onboarding and annually thereafter.	Inspected the code of conduct and code of conduct acknowledgement for a sample of new hires and current employees to determine that the Company maintained a documented Code of Conduct, and eligible personnel were required to accept the Company's Code of Conduct during onboarding and annually thereafter.	No exceptions noted.
		The Company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role.	Inspected the job description for a sample of job roles to determine that the Company had documented job descriptions for each position at the company, which included roles and responsibilities as well as required qualifications, skills, and experience for the role.	No exceptions noted.
		The Company has a defined disciplinary sanctions process to be enacted when a member of the workforce violates the Company's policies or causes a security or privacy incident. Management retains documentation of instances when the disciplinary process was enacted.	Inquired of the VP, Information Security and IT regarding the disciplinary process to determine that the company had a defined disciplinary process to be enacted when a member of the workforce violated the company's policies or caused a security or privacy incident, and management retained documentation of instances when the disciplinary process was enacted.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the code of conduct to determine that the Company had a defined disciplinary sanctions process to be enacted when a member of the workforce violated the Company's policies or caused a security or privacy incident. Management retained documentation of instances when the disciplinary process was enacted.	No exceptions noted.
			Inspected the HR records to determine that the Company had a defined disciplinary sanctions process to be enacted when a member of the workforce violated the Company's policies or caused a security or privacy incident, and management retained documentation of instances when the disciplinary process was enacted.	Testing of the control activity disclosed that there were no instances where a member of the workforce violated the company's policies or caused a security or privacy incident during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The Company has defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	Inspected the information security policies and topic-specific policies to determine that the Company had defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	No exceptions noted.
		A documented network diagram is in place to document system boundaries and connections to external networks. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment.	Inspected the network diagram, including the version history, to determine that a documented network diagram was in place to document system boundaries and connections to external networks, and the network diagram was reviewed and approved by management at least annually and updated as necessary when there were changes to the environment.	No exceptions noted.
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Inspected the compliance automation software and information security policy acknowledgements for a sample of new hires and current employees to determine that Company policies were accessible to all employees and, as applicable, third-parties such as contractors, and personnel were required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary.	Inspected the information security policies version history and records of approvals to determine that management reviewed and approved company policies at least annually, and updates to the policies were made as deemed necessary.	No exceptions noted.
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the segregated VPCs and the associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.
		Cloud resources are configured to deny public access.	Inspected the VPC security groups and associated inbound and outbound rules to determine that cloud resources were configured to deny public access.	No exceptions noted.
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the network diagram and VPC security groups and associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected the network diagram and IDS configurations to determine that an IDS was in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and was configured to alert personnel when a potential intrusion was detected.	No exceptions noted.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The Company has defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	Inspected the information security policies and topic-specific policies to determine that the Company had defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	No exceptions noted.
		The company's board of directors meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented.	Inspected the internal controls and operations review management meeting minutes to determine that the Company's board of directors met at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies, and meeting minutes, including decisions made and action items, were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel responsibilities for information security are communicated to and acknowledged by personnel.	Inquired of the VP, Security and IT Operations regarding the onboarding process to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
			Inspected the company policy acknowledgment for a sample of new hires to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Inspected the compliance automation software and information security policy acknowledgements for a sample of new hires and current employees to determine that Company policies were accessible to all employees and, as applicable, third-parties such as contractors, and personnel were required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary.	Inspected the information security policies version history and records of approvals to determine that management reviewed and approved company policies at least annually, and updates to the policies were made as deemed necessary.	No exceptions noted.
		The Company has established training programs to help personnel gain awareness of information security best practices. Personnel are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary.	Inspected the information security policies and procedures and training completion certificates for a sample of new hires and current employees to determine that the Company had established training programs to help personnel gain awareness of information security best practices, personnel were required to complete the training during onboarding, and periodic refresher training is provided to personnel at least annually and as deemed necessary.	No exceptions noted.
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the information security policies and procedures, organizational chart, compliance automation software, and job description for a sample of job roles to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company maintains a documented Code of Conduct. Eligible personnel are required to accept the Company's Code of Conduct during onboarding and annually thereafter.	Inspected the code of conduct and code of conduct acknowledgement for a sample of new hires and current employees to determine that the Company maintained a documented Code of Conduct, and eligible personnel were required to accept the Company's Code of Conduct during onboarding and annually thereafter.	No exceptions noted.
		The Company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role.	Inspected the job description for a sample of job roles to determine that the Company had documented job descriptions for each position at the company, which included roles and responsibilities as well as required qualifications, skills, and experience for the role.	No exceptions noted.
		The Company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs.	Inquired of the VP, Security and IT Operations regarding customer support issues to determine that the company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident management and escalation policies and procedures to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the entity's website to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the supporting ticket for a sample of customer support issues to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	Testing of the control activity disclosed that there were no customer support issues reported during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.	Inspected the company's website, compliance automation software, code of conduct, internal communication channel and incident management and escalation policies and procedures to determine that internal communication channels were in place for employees to report failures, events, incidents, concerns, and other issues to company management.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's board of directors meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented.	Inspected the internal controls and operations review management meeting minutes to determine that the Company's board of directors met at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies, and meeting minutes, including decisions made and action items, were documented.	No exceptions noted.
		Personnel responsibilities for information security are communicated to and acknowledged by personnel.	Inquired of the VP, Security and IT Operations regarding the onboarding process to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the company policy acknowledgment for a sample of new hires to determine that personnel responsibilities for information security, were communicated to and acknowledged by personnel.	No exceptions noted.
		The Company maintains a third-party register that includes a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc. The Company executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider.	Inspected the third-party register to determine that the Company maintained a third-party register that included a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc., and the Company executed agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outlined the responsibilities of each vendor or service provider.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the third-party agreement for a sample of third-parties to determine that the Company maintained a third-party register that included a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc., and the Company executed agreements with third-party and service providers involved in accessing, processing, storing or managing information assets that outlined the responsibilities of each third-party and service provider.	No exceptions noted.
		The company maintains a publicly available ToS for use of the system. All users must agree to the ToS prior to using the system.	Inspected the company's website and the publicly available ToS to determine that the company maintained a publicly available ToS for use of the system, and users had to agree to the ToS prior to using the system.	No exceptions noted.
		The Company communicates service commitments and system requirements to customers through contracts, agreements, company website, etc. The Company provides notification to relevant parties of any changes to service commitments and system requirements.	Inquired of the VP, Security and IT Operations regarding customers to determine that the Company communicated service commitments and system requirements to customers through contracts, agreements, company website, etc., and the Company provided notification to relevant parties of any changes to services commitments and system requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the information security policies and standard operating procedures to determine that the Company communicated service commitments and system requirements to customers through contracts, agreements, company website, etc., and the Company provided notification to relevant parties of any changes to services commitments and system requirements.	No exceptions noted.
			Inspected the customer agreement for a sample of customers to determine that the Company communicated service commitments and system requirements to customers through contracts, agreements, company website, etc., and the Company provided notification to relevant parties of any changes to services commitments and system requirements.	Testing of the control activity disclosed that there were no active customers during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company provides user guides, help articles, system documentation or other mechanisms to users to share information about the design and operation of the system and its boundaries. The information provided includes functional and nonfunctional requirements related to system processing and information specifications required to support the use of the system.	Inspected the company website and user guides to determine that the Company provided user guides, help articles, system documentation or other mechanisms to users to share information about the design and operation of the system and its boundaries, and the information provided included functional and nonfunctional requirements related to system processing and information specifications required to support the use of the system.	No exceptions noted.
		The Company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs.	Inquired of the VP, Security and IT Operations regarding customer support issues to determine that the company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the incident management and escalation policies and procedures to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the entity's website to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the supporting ticket for a sample of customer support issues to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	Testing of the control activity disclosed that there were no customer support issues reported during the review period.
		Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.	Inspected the company's website, compliance automation software, code of conduct, internal communication channel and incident management and escalation policies and procedures to determine that internal communication channels were in place for employees to report failures, events, incidents, concerns, and other issues to company management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The Company has defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	Inspected the information security policies and topic-specific policies to determine that the Company had defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	No exceptions noted.
		An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees and is updated upon changes to the organizational structure.	Inspected the organizational chart, including the revision history to determine that an organizational chart was in place to describe the organizational structure and reporting lines, and the chart was available to all employees and was updated upon changes to the organizational structure.	No exceptions noted.
		The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Inspected the compliance automation software and information security policy acknowledgements for a sample of new hires and current employees to determine that Company policies were accessible to all employees and, as applicable, third-parties such as contractors, and personnel were required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.
		Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary.	Inspected the information security policies version history and records of approvals to determine that management reviewed and approved company policies at least annually, and updates to the policies were made as deemed necessary.	No exceptions noted.
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the information security policies and procedures, organizational chart, compliance automation software, and job description for a sample of job roles to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company communicates service commitments and system requirements to customers through contracts, agreements, company website, etc. The Company provides notification to relevant parties of any changes to service commitments and system requirements.	Inquired of the VP, Security and IT Operations regarding customers to determine that the Company communicated service commitments and system requirements to customers through contracts, agreements, company website, etc., and the Company provided notification to relevant parties of any changes to services commitments and system requirements.	No exceptions noted.
			Inspected the information security policies and standard operating procedures to determine that the Company communicated service commitments and system requirements to customers through contracts, agreements, company website, etc., and the Company provided notification to relevant parties of any changes to services commitments and system requirements.	No exceptions noted.
			Inspected the customer agreement for a sample of customers to determine that the Company communicated service commitments and system requirements to customers through contracts, agreements, company website, etc., and the Company provided notification to relevant parties of any changes to services commitments and system requirements.	Testing of the control activity disclosed that there were no active customers during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has defined company objectives, including mission and vision statements, operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate, to serve as the basis for risk assessment activities. Management communicates its objectives and any changes to those objectives to personnel.	Inspected the annual management internal controls review meeting minutes and compliance automation software to determine that management had defined company objectives, including mission and vision statements, operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate, to serve as the basis for risk assessment activities and management communicated its objectives and any changes to those objectives to personnel.	No exceptions noted.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
		The Company performs due diligence activities prior to engaging with a new service provider or vendor. Results of the due diligence activities including action items are documented.	Inspected the vendor listing and completed supplier evaluation form for a sample of third-parties to determine that the Company performed due diligence activities prior to engaging with a new service provider or vendor, and the results of the due diligence activities including action items were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, are documented.	Inspected the compliance reports and associated security review documentation for a sample of third-parties to determine that the Company obtained and reviewed compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, were documented.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
		The Company performs an evaluation of fraud risks at least annually, either as a separate evaluation or as part of the overall enterprise risk assessment. The evaluation of fraud risk is performed in accordance with the company's risk assessment methodology.	Inspected the completed risk assessment to determine that the Company performed an evaluation of fraud risks at least annually, either as a separate evaluation or as part of the overall enterprise risk assessment, and the evaluation of fraud risk was performed in accordance with the company's risk assessment methodology.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
		The Company performs due diligence activities prior to engaging with a new service provider or vendor. Results of the due diligence activities including action items are documented.	Inspected the vendor listing and completed supplier evaluation form for a sample of third-parties to determine that the Company performed due diligence activities prior to engaging with a new service provider or vendor, and the results of the due diligence activities including action items were documented.	No exceptions noted.
		The Company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, are documented.	Inspected the compliance reports and associated security review documentation for a sample of third-parties to determine that the Company obtained and reviewed compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Changes to the entity's systems, applications, technologies, tools, and leadership are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that changes to the entity's systems, applications, technologies, tools, and leadership were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Management performs user access reviews annually to validate user accounts, including Third-party, and their associated privileges remain appropriate. The review includes validation of logical as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected the completed network user access review, application user access review, database user access review, operating system user access review to determine that management performed user access reviews annually to validate user accounts, including third-party, and their associated privileges remained appropriate, the review included validation of logical as necessary, and changes resulting from the review, if any, were documented and implemented.	No exceptions noted.
		The Company has defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	Inspected the information security policies and topic-specific policies to determine that the Company had defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company conducts monthly vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies.	Inspected the completed vulnerability scan results for a sample of months and the associated resolution documentation for a sample of critical and high-risk vulnerabilities identified from a vulnerability scan to determine that the Company conducted monthly vulnerability scans of the production environment as dictated by company policy and compliance requirements, and the results were reviewed by company personnel and vulnerabilities were tracked to resolution in accordance with company policies.	No exceptions noted.
		The company has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	Inspected the vulnerability management policies and procedures to determine that the company had a defined policy that established requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An external penetration test of production environments is performed by an independent third-party annually or after any significant infrastructure or application changes. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies.	Inspected the completed penetration test results and associated resolution documentation for a sample of high-risk vulnerabilities identified from a penetration test to determine that an external penetration test of production environments was performed by an independent third-party annually or after any significant infrastructure or application changes, and the results were reviewed by management and vulnerabilities were tracked to resolution in accordance with company policies.	No exceptions noted.
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Inspected the compliance automation software and information security policy acknowledgements for a sample of new hires and current employees to determine that Company policies were accessible to all employees and, as applicable, third-parties such as contractors, and personnel were required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary.	Inspected the information security policies version history and records of approvals to determine that management reviewed and approved company policies at least annually, and updates to the policies were made as deemed necessary.	No exceptions noted.
		Management conducts annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	Inspected the code of conduct and completed performance and conduct evaluation form for a sample of current employees to determine that management conducted annual evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.	No exceptions noted.
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the information security policies and procedures, organizational chart, compliance automation software, and job description for a sample of job roles to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company performs due diligence activities prior to engaging with a new service provider or vendor. Results of the due diligence activities including action items are documented.	Inspected the vendor listing and completed supplier evaluation form for a sample of third-parties to determine that the Company performed due diligence activities prior to engaging with a new service provider or vendor, and the results of the due diligence activities including action items were documented.	No exceptions noted.
		The Company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, are documented.	Inspected the compliance reports and associated security review documentation for a sample of third-parties to determine that the Company obtained and reviewed compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production systems and resources are monitored and automated alerts are sent out personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary.	Inspected the monitoring tool configurations, the anti-malware software dashboard console, source code repository configurations, IDS configurations, firewall rule sets for a sample of production servers, and the anti-malware, source code repository, and IDS alert configurations and an example alert to determine that production systems and resources were monitored and automated alerts were sent out personnel based on pre-configured rules, and events were triaged to determine if they constituted an incident and escalated per policy if necessary.	No exceptions noted.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company's board of directors meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented.	Inspected the internal controls and operations review management meeting minutes to determine that the Company's board of directors met at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies, and meeting minutes, including decisions made and action items, were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the information security policies and procedures, organizational chart, compliance automation software, and job description for a sample of job roles to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
		The Company has a defined Business Continuity Plan that outlines strategies for maintaining operations during a disruption.	Inspected the business continuity plans to determine that the Company had a defined Business Continuity Plan that outlined strategies for maintaining operations during a disruption.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
		The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	Inspected the disaster recovery plans to determine that the Company had a documented disaster recovery plan that outlined roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company conducts tests of the business continuity and disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary.	Inspected the completed business continuity and disaster recovery test results to determine that the Company conducted tests of the business continuity and disaster recovery plans at least annually, the results and lessons learned were documented, and updates to the plans were made as necessary.	No exceptions noted.
		The board of directors includes members independent from management who are not involved in control operations.	Inspected the board charter and board meeting minutes to determine that the board of directors included members independent from management who were not involved in control operations.	No exceptions noted.
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the information security policies and procedures, organizational chart, compliance automation software, and job description for a sample of job roles to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The Company has defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	Inspected the information security policies and topic-specific policies to determine that the Company had defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	No exceptions noted.
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Inspected the compliance automation software and information security policy acknowledgements for a sample of new hires and current employees to determine that Company policies were accessible to all employees and, as applicable, third-parties such as contractors, and personnel were required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary.	Inspected the information security policies version history and records of approvals to determine that management reviewed and approved company policies at least annually, and updates to the policies were made as deemed necessary.	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The Company has defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	Inspected the information security policies and topic-specific policies to determine that the Company had defined and documented an Information Security Policy and other topic-specific policies to support the functioning of internal control.	No exceptions noted.
		The Company uses compliance automation software to identify, select, and continuously monitor internal controls.	Inspected the compliance automation software to determine that the Company used compliance automation software to identify, select, and continuously monitor internal controls.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Company policies are accessible to all employees and, as applicable, third-parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	Inspected the compliance automation software and information security policy acknowledgements for a sample of new hires and current employees to determine that Company policies were accessible to all employees and, as applicable, third-parties such as contractors, and personnel were required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.	No exceptions noted.
		Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary.	Inspected the information security policies version history and records of approvals to determine that management reviewed and approved company policies at least annually, and updates to the policies were made as deemed necessary.	No exceptions noted.
		Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	Inspected the information security policies and procedures, organizational chart, compliance automation software, and job description for a sample of job roles to determine that management had defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has documented job descriptions for each position at the company, which include roles and responsibilities as well as required qualifications, skills, and experience for the role.	Inspected the job description for a sample of job roles to determine that the Company had documented job descriptions for each position at the company, which included roles and responsibilities as well as required qualifications, skills, and experience for the role.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
		Management performs user access reviews annually to validate user accounts, including Third-party, and their associated privileges remain appropriate. The review includes validation of logical as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected the completed network user access review, application user access review, database user access review, operating system user access review to determine that management performed user access reviews annually to validate user accounts, including third-party, and their associated privileges remained appropriate, the review included validation of logical as necessary, and changes resulting from the review, if any, were documented and implemented.	No exceptions noted.
		A centralized asset register is maintained for physical, cloud, and other assets that includes descriptive attributes for asset accountability such as owner, description, location, classification, and other information based on the type of asset. Processes are in place to maintain an updated inventory through automated mechanisms.	Inspected the inventory listing of system assets and components, including the revision history, and compliance automation software to determine that a centralized asset register was maintained for physical, cloud, and other assets that included descriptive attributes for asset accountability such as owner, description, location, classification, and other information based on the type of asset, and processes were in place to maintain an updated inventory through automated mechanisms.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Key-management policies and procedures are documented and implemented including: generation of strong cryptographic keys, secure distribution, and secure storage of cryptographic keys used to protect sensitive data.	Inspected the encryption policies and procedures to determine that key-management policies and procedures were documented and implemented including: generation of strong cryptographic keys, secure distribution, and secure storage of cryptographic keys used to protect sensitive data.	No exceptions noted.
		The Company retires, replaces or destructs cryptographic keys that are no longer used or needed or when the key expires, the integrity of the key has been weakened, or the key is known or suspected to be compromised, in accordance with documented company policies and procedures. Retired or replaced keys are not used for encryption operations.	Inspected the encryption policies and procedures to determine that the Company retired, replaced or destructed cryptographic keys that were no longer used or needed or when the key expired, the integrity of the key was weakened, or the key was known or suspected to be compromised, in accordance with documented company policies and procedures, and retired or replaced keys were not used for encryption operations.	No exceptions noted.
		The Company restricts access to system components and data to only those individuals whose job requires such access.	Inquired of the VP, Security and IT Operations regarding access to system components and sensitive data to determine that the Company restricted access to system components and data to only those individuals whose job required such access.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the network, application, database, operating system user listings and access rights to determine that the Company restricted access to system components and data to only those individuals whose job required such access.	No exceptions noted.
		Invalid authentication attempts are limited by locking out the user ID after not more than 5 failed attempts.	Inspected the internal network account lockout settings to determine that invalid authentication attempts were limited by locking out the user ID after not more than 5 failed attempts.	No exceptions noted.
		The Company has configured account lockout duration following a set number of invalid authentication attempts to a minimum of 60 minutes or until the identity of the user is confirmed.	Inspected the internal network account lockout duration settings to determine that the Company had configured account lockout duration following a set number of invalid authentication attempts to a minimum of 60 minutes or until the identity of the user was confirmed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.
		Audit logs are enabled and active for system components and sensitive data in accordance with company policies.	Inspected the information security and logging and monitoring policies and procedures and network, application, database and operating system audit logging settings and an example audit log extract to determine that audit logs were enabled and active for system components and sensitive data in accordance with company policies.	No exceptions noted.
		Data at rest is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data at rest to determine that data at rest was encrypted using strong cryptographic algorithms.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data in transit is encrypted using strong cryptographic algorithms.	Inspected encryption configurations for data in transit to determine that data in transit was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Group, shared, or generic account usage is prevented unless strictly necessary and supported by documented business justification and management approval. Mechanisms are in place to confirm individual user identity before access to the account is granted and to trace every action to an individual user.	Inquired of the VP, Security and IT Operations regarding group, shared, or generic account usage to determine that group, shared, or generic account usage was prevented unless strictly necessary and supported by documented business justification and management approval, and mechanisms were in place to confirm individual user identity before access to the account was granted and to trace every action to an individual user.	No exceptions noted.
			Inspected the system access control policies and procedures to determine that group, shared, or generic account usage was prevented unless strictly necessary and supported by documented business justification and management approval, and mechanisms were in place to confirm individual user identity before access to the account was granted and to trace every action to an individual user.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the network, application, database and operating system user listings and access rights to determine that group, shared, or generic account usage was prevented unless strictly necessary and supported by documented business justification and management approval, and mechanisms were in place to confirm individual user identity before access to the account was granted and to trace every action to an individual user.	Testing of the control activity disclosed that there were no group, shared, or generic accounts used during the review period.
		Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.	Inquired of the VP, Security and IT Operations regarding privileged access to determine that administrative or privileged access to systems, resources, and functions was restricted to authorized personnel.	No exceptions noted.
			Inspected the network, application, database and operating system administrator listings and access rights as well as the administrator listings and access rights to determine that administrative or privileged access to systems, resources, and functions was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has implemented technical measures to protect stored user passwords for the system.	Inspected the encryption configurations for stored user passwords to determine that the Company had implemented technical measures to protect stored user passwords for the system.	No exceptions noted.
		The Company has implemented segregation controls so that customers cannot impact or access data or resources of other customers.	Inspected the network diagram to determine that the Company had implemented segregation controls so that customers could not impact or access data or resources of other customers.	No exceptions noted.
		The Company has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy.	Inspected the system access control policies and procedures, and password configurations for the network, application, database and operating system layers and the systems storing ePHI to determine that the Company had a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems, and password requirements were enforced for all systems in accordance with company policy.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Inspected the system access control policies and procedures, network, application, database, and operating system listings, and the user access request ticket for a sample of new hires to determine that access requests to information resources, including access to systems and data, were documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.
		System access is revoked within one business day of effective termination date for terminated users.	Inspected the system access control policies and procedures, network, application, database, and operating system listings, and the user access revocation ticket for a sample of terminated employees to determine that system and physical access was revoked within one business day of effective termination date for terminated users.	No exceptions noted.
		Authentication to systems requires the use of unique identities.	Inspected the network, application, database and operating system user listings and access rights to determine that authentication to systems required the use of unique identities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Root password authentication to production resources is disabled and only allowed for under exceptional circumstances for a limited time duration based on documented business justification and approval from management.	Inspected the system access control policies and procedures and root password authentication settings for the productions instance to determine that root password authentication to production resources was disabled and only allowed for under exceptional circumstances for a limited time duration based on documented business justification and approval from management.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.
		The company uses network segmentation and other techniques to isolate portions of the environment and to control traffic between them based on security and business needs.	Inspected the network diagram, and the firewall rule sets for a sample of production servers to determine that the company used network segmentation and other techniques to isolate portions of the environment and to control traffic between them based on security and business needs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company uses a centralized system that collects and stores logs of system activity and sends alerts to personnel based on pre-configured rules. Access to logs is restricted to authorized personnel.	Inquired of the VP, Security and IT Operations regarding access to audit logs to determine that the Company used a centralized system that collected and stored logs of system activity and sent alerts to personnel based on pre-configured rules, and access to logs was restricted to authorized personnel.	No exceptions noted.
			Inspected the network, application, database, and operating system audit logging access listings and an example audit log extract to determine that the Company used a centralized system that collected and stored logs of system activity and sent alerts to personnel based on pre-configured rules, and access to logs was restricted to authorized personnel.	No exceptions noted.
		Access to the root account in the cloud infrastructure provider is monitored. Login activity for the root account is investigated and validated for appropriateness.	Inspected the compliance automation software and supporting login documentation to determine that access to the root account in the cloud infrastructure provider was monitored, and login activity for the root account was investigated and validated for appropriateness.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
		Management performs user access reviews annually to validate user accounts, including Third-party, and their associated privileges remain appropriate. The review includes validation of logical as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected the completed network user access review, application user access review, database user access review, operating system user access review to determine that management performed user access reviews annually to validate user accounts, including third-party, and their associated privileges remained appropriate, the review included validation of logical as necessary, and changes resulting from the review, if any, were documented and implemented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.
		Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Inspected the system access control policies and procedures, network, application, database, and operating system listings, and the user access request ticket for a sample of new hires to determine that access requests to information resources, including access to systems and data, were documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System access is revoked within one business day of effective termination date for terminated users.	Inspected the system access control policies and procedures, network, application, database, and operating system listings, and the user access revocation ticket for a sample of terminated employees to determine that system and physical access was revoked within one business day of effective termination date for terminated users.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	The Company has developed and documented a policy that outlines requirements for access control.	Inspected the system access control policies and procedures to determine that the Company had developed and documented a policy that outlined requirements for access control.	No exceptions noted.
		Management performs user access reviews annually to validate user accounts, including Third-party, and their associated privileges remain appropriate. The review includes validation of logical as necessary. Changes resulting from the review, if any, are documented and implemented.	Inspected the completed network user access review, application user access review, database user access review, operating system user access review to determine that management performed user access reviews annually to validate user accounts, including third-party, and their associated privileges remained appropriate, the review included validation of logical as necessary, and changes resulting from the review, if any, were documented and implemented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has documented policies and procedures for authentication that are communicated to all personnel. These documents include guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	Inspected the system access control policies and procedures, password policies and procedures and compliance automation software to determine that the Company had documented policies and procedures for authentication that were communicated to all personnel, and that these documents included guidance on selecting strong authentication factors, guidance on protecting authentication credentials, instructions not to reuse previously used credentials, instructions to change authentication credentials in the event of known or suspected compromise along with guidance on how to report the incident, etc.	No exceptions noted.
		Access requests to information resources, including access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles.	Inspected the system access control policies and procedures, network, application, database, and operating system listings, and the user access request ticket for a sample of new hires to determine that access requests to information resources, including access to systems and data, were documented and approved by management based on least privilege, need to know, and segregation of duties principles.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System access is revoked within one business day of effective termination date for terminated users.	Inspected the system access control policies and procedures, network, application, database, and operating system listings, and the user access revocation ticket for a sample of terminated employees to determine that system and physical access was revoked within one business day of effective termination date for terminated users.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not Applicable.	Not Applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The Company disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	Inquired of the VP, Security and IT Operations, regarding data disposal to determine that the company disposed of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the data deletion policies and procedures to determine that the Company disposed of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	No exceptions noted.
			Inspected the destruction certificate for a sample of requests to dispose of data on hardware to determine that the Company disposed of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.	Testing of the control activity disclosed that there no requests to dispose of data occurred during the review period.
		The Company has documented policies and procedures for erasure or destruction of information that has been identified for disposal.	Inspected the data retention policies and procedures to determine that the company had documented and implemented policies and procedures for erasure or destruction of information that has been identified for disposal.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The deployed anti-malware solution is kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	Inspected the anti-malware settings to determine that the deployed anti-malware solution was kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The implemented anti-malware solutions are configured to perform real-time scans.	Inspected the anti-malware settings to determine that the implemented anti-malware solutions were configured to perform real-time scans.	No exceptions noted.
		The Company restricts access to system components and data to only those individuals whose job requires such access.	Inquired of the VP, Security and IT Operations regarding access to system components and sensitive data to determine that the Company restricted access to system components and data to only those individuals whose job required such access.	No exceptions noted.
			Inspected the network, application, database, operating system user listings and access rights to determine that the Company restricted access to system components and data to only those individuals whose job required such access.	No exceptions noted.
		Anti-malware software is installed on company-managed devices.	Inspected the anti-malware software dashboard console to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.
			Inspected the anti-malware settings for a sample of devices to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data at rest is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data at rest to determine that data at rest was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Data in transit is encrypted using strong cryptographic algorithms.	Inspected encryption configurations for data in transit to determine that data in transit was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the segregated VPCs and the associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.
		Cloud resources are configured to deny public access.	Inspected the VPC security groups and associated inbound and outbound rules to determine that cloud resources were configured to deny public access.	No exceptions noted.
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the network diagram and VPC security groups and associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	Inspected the threat detection system and an example alert to determine that a threat detection system was in place to monitor web traffic and suspicious activity, and when anomalous traffic activity was identified, alerts were automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	No exceptions noted.
		A web-application firewall (WAF) is in place to protect public-facing web applications from outside threats.	Inspected the network diagram to determine that a WAF was in place to protect public-facing web applications from outside threats.	No exceptions noted.
			Inspected the WAF configurations for the production server to determine that a WAF was in place to protect public-facing web applications from outside threats.	No exceptions noted.
		An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected the network diagram and IDS configurations to determine that an IDS was in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and was configured to alert personnel when a potential intrusion was detected.	No exceptions noted.
		Remote access to production systems is only available through an encrypted connection.	Inspected the encryption configurations to determine that remote access to production systems was only available through an encrypted connection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Automated backups of critical systems are performed on at least a daily basis.	Inspected the backup policies and procedures to determine that automated backups were performed on at least a daily basis.	No exceptions noted.
			Inspected the automated backup configurations and the automated backup log for a sample of days to determine that the automated backups were performed on at least a daily basis.	No exceptions noted.
		The Company restricts access to system components and data to only those individuals whose job requires such access.	Inquired of the VP, Security and IT Operations regarding access to system components and sensitive data to determine that the Company restricted access to system components and data to only those individuals whose job required such access.	No exceptions noted.
			Inspected the network, application, database, operating system user listings and access rights to determine that the Company restricted access to system components and data to only those individuals whose job required such access.	No exceptions noted.
		Data at rest is encrypted using strong cryptographic algorithms.	Inspected the encryption configurations for data at rest to determine that data at rest was encrypted using strong cryptographic algorithms.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data in transit is encrypted using strong cryptographic algorithms.	Inspected encryption configurations for data in transit to determine that data in transit was encrypted using strong cryptographic algorithms.	No exceptions noted.
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the segregated VPCs and the associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.
		Cloud resources are configured to deny public access.	Inspected the VPC security groups and associated inbound and outbound rules to determine that cloud resources were configured to deny public access.	No exceptions noted.
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the network diagram and VPC security groups and associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.
		A WAF is in place to protect public-facing web applications from outside threats.	Inspected the network diagram to determine that a WAF was in place to protect public-facing web applications from outside threats.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the WAF configurations for the production server to determine that a WAF was in place to protect public-facing web applications from outside threats.	No exceptions noted.
		An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected the network diagram and IDS configurations to determine that an IDS was in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and was configured to alert personnel when a potential intrusion was detected.	No exceptions noted.
		Remote access to production systems is only available through an encrypted connection.	Inspected the encryption configurations to determine that remote access to production systems was only available through an encrypted connection.	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 deployed anti-malware solution is kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	Inspected the anti-malware settings to determine that the deployed anti-malware solution was kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	No exceptions noted.
		The implemented anti-malware solutions are configured to perform real-time scans.	Inspected the anti-malware settings to determine that the implemented anti-malware solutions were configured to perform real-time scans.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Changes to system components in the production environment are made according to established procedures that include documentation and testing.	Inspected the change management policies and procedures to determine that changes to system components in the production environment were made according to established procedures that included documentation and testing.	No exceptions noted.
			Inspected the supporting change ticket for a sample of system and infrastructure changes to determine that changes to system components in the production environment were made according to established procedures that included documentation and testing.	No exceptions noted.
		The company has enabled change-detection mechanism to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected the source code repository configurations to determine that the company had enabled change-detection mechanism to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data could not be changed without generating alerts.	No exceptions noted.
		Anti-malware software is installed on company-managed devices.	Inspected the anti-malware software dashboard console to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the anti-malware settings for a sample of devices to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.
		Access to make changes in production environments is restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures.	Inquired of the VP, Security and IT Operations regarding the ability to migrate changes into the production environment to determine that access to make changes in production environments was restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures.	No exceptions noted.
			Inspected the list of users with the ability to deploy changes into the production environment to determine that access to make changes in production environments was restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production systems and resources are monitored and automated alerts are sent out personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary.	Inspected the monitoring tool configurations, the anti-malware software dashboard console, source code repository configurations, IDS configurations, firewall rule sets for a sample of production servers, and the anti-malware, source code repository, and IDS alert configurations and an example alert to determine that production systems and resources were monitored and automated alerts were sent out personnel based on pre-configured rules, and events were triaged to determine if they constituted an incident and escalated per policy if necessary.	No exceptions noted.
		A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	Inspected the threat detection system and an example alert to determine that a threat detection system was in place to monitor web traffic and suspicious activity, and when anomalous traffic activity was identified, alerts were automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The Company has identified and documented baseline security configuration standards for system components in accordance with industry-accepted hardening standards or vendor recommendations. These standards are reviewed at least annually and updated as needed and verified to be in place before or immediately after a production system component is installed or modified.	Inspected the asset management policies and procedures and documented baseline security configuration standards, including the revision history, to determine that the Company had identified and documented baseline security configuration standards for system components in accordance with industry-accepted hardening standards or vendor recommendations, and these standards were reviewed at least annually and updated as needed and verified to be in place before or immediately after a production system component was installed or modified.	No exceptions noted.
		The Company conducts monthly vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies.	Inspected the completed vulnerability scan results for a sample of months and the associated resolution documentation for a sample of critical and high-risk vulnerabilities identified from a vulnerability scan to determine that the Company conducted monthly vulnerability scans of the production environment as dictated by company policy and compliance requirements, and the results were reviewed by company personnel and vulnerabilities were tracked to resolution in accordance with company policies.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The company has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	Inspected the vulnerability management policies and procedures to determine that the company had a defined policy that established requirements for vulnerability management across the organization, including monitoring, cataloguing, and assigning risk ratings to vulnerabilities to prioritize remediation efforts.	No exceptions noted.
		An external penetration test of production environments is performed by an independent third-party annually or after any significant infrastructure or application changes. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies.	Inspected the completed penetration test results and associated resolution documentation for a sample of high-risk vulnerabilities identified from a penetration test to determine that an external penetration test of production environments was performed by an independent third-party annually or after any significant infrastructure or application changes, and the results were reviewed by management and vulnerabilities were tracked to resolution in accordance with company policies.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The company has enabled change-detection mechanism to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected the source code repository configurations to determine that the company had enabled change-detection mechanism to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data could not be changed without generating alerts.	No exceptions noted.
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the segregated VPCs and the associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.
		Cloud resources are configured to deny public access.	Inspected the VPC security groups and associated inbound and outbound rules to determine that cloud resources were configured to deny public access.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Storage buckets that contain sensitive data have versioning enabled to preserve, retrieve, and restore versions of objects.	Inspected the object versioning settings to determine that storage buckets that contained sensitive data had versioning enabled to preserve, retrieve, and restore versions of objects.	No exceptions noted.
		Management has defined company objectives, including mission and vision statements, operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate, to serve as the basis for risk assessment activities. Management communicates its objectives and any changes to those objectives to personnel.	Inspected the annual management internal controls review meeting minutes and compliance automation software to determine that management had defined company objectives, including mission and vision statements, operational objectives at the entity and functional levels, financial performance goals, and other objectives as appropriate, to serve as the basis for risk assessment activities and management communicated its objectives and any changes to those objectives to personnel.	No exceptions noted.
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the network diagram and VPC security groups and associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production systems and resources are monitored and automated alerts are sent out personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary.	Inspected the monitoring tool configurations, the anti-malware software dashboard console, source code repository configurations, IDS configurations, firewall rule sets for a sample of production servers, and the anti-malware, source code repository, and IDS alert configurations and an example alert to determine that production systems and resources were monitored and automated alerts were sent out personnel based on pre-configured rules, and events were triaged to determine if they constituted an incident and escalated per policy if necessary.	No exceptions noted.
		A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	Inspected the threat detection system and an example alert to determine that a threat detection system was in place to monitor web traffic and suspicious activity, and when anomalous traffic activity was identified, alerts were automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	No exceptions noted.
		A WAF is in place to protect public-facing web applications from outside threats.	Inspected the network diagram to determine that a WAF was in place to protect public-facing web applications from outside threats.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the WAF configurations for the production server to determine that a WAF was in place to protect public-facing web applications from outside threats.	No exceptions noted.
		An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected the network diagram and IDS configurations to determine that an IDS was in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and was configured to alert personnel when a potential intrusion was detected.	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 deployed anti-malware solution is kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	Inspected the anti-malware settings to determine that the deployed anti-malware solution was kept current via automatic updates and configured to detect all known types of malware and to remove, block, or contain all known types of malware.	No exceptions noted.
		The implemented anti-malware solutions are configured to perform real-time scans.	Inspected the anti-malware settings to determine that the implemented anti-malware solutions were configured to perform real-time scans.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Audit logs are enabled and active for system components and sensitive data in accordance with company policies.	Inspected the information security and logging and monitoring policies and procedures and network, application, database and operating system audit logging settings and an example audit log extract to determine that audit logs were enabled and active for system components and sensitive data in accordance with company policies.	No exceptions noted.
		The company has enabled change-detection mechanism to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected the source code repository configurations to determine that the company had enabled change-detection mechanism to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data could not be changed without generating alerts.	No exceptions noted.
		Anti-malware software is installed on company-managed devices.	Inspected the anti-malware software dashboard console to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.
			Inspected the anti-malware settings for a sample of devices to determine that anti-malware software was installed on company-managed devices.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the segregated VPCs and the associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.
		The Company has a documented policy that outlines requirements for audit logging and monitoring of system activity at the company.	Inspected the information security policies and procedures and logging and monitoring policies and procedures to determine that the Company had a documented policy that outlined requirements for audit logging and monitoring of system activity at the company.	No exceptions noted.
		Cloud resources are configured to deny public access.	Inspected the VPC security groups and associated inbound and outbound rules to determine that cloud resources were configured to deny public access.	No exceptions noted.
		The Company uses a centralized system that collects and stores logs of system activity and sends alerts to personnel based on pre-configured rules. Access to logs is restricted to authorized personnel.	Inquired of the VP, Security and IT Operations regarding access to audit logs to determine that the Company used a centralized system that collected and stored logs of system activity and sent alerts to personnel based on pre-configured rules, and access to logs was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the network, application, database, and operating system audit logging access listings and an example audit log extract to determine that the Company used a centralized system that collected and stored logs of system activity and sent alerts to personnel based on pre-configured rules, and access to logs was restricted to authorized personnel.	No exceptions noted.
		The Company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs.	Inquired of the VP, Security and IT Operations regarding customer support issues to determine that the company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the incident management and escalation policies and procedures to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the entity's website to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the supporting ticket for a sample of customer support issues to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	Testing of the control activity disclosed that there were no customer support issues reported during the review period.
		Network security configurations are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inspected the network diagram and VPC security groups and associated inbound and outbound rules to determine that network security configurations were in place to limit inbound and outbound traffic to the environment to only what was necessary based on business justification, and all other traffic was specifically denied.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production systems and resources are monitored and automated alerts are sent out personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary.	Inspected the monitoring tool configurations, the anti-malware software dashboard console, source code repository configurations, IDS configurations, firewall rule sets for a sample of production servers, and the anti-malware, source code repository, and IDS alert configurations and an example alert to determine that production systems and resources were monitored and automated alerts were sent out personnel based on pre-configured rules, and events were triaged to determine if they constituted an incident and escalated per policy if necessary.	No exceptions noted.
		A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	Inspected the threat detection system and an example alert to determine that a threat detection system was in place to monitor web traffic and suspicious activity, and when anomalous traffic activity was identified, alerts were automatically sent to personnel, investigated, and escalated through the incident management process, if necessary.	No exceptions noted.
		A WAF is in place to protect public-facing web applications from outside threats.	Inspected the network diagram to determine that a WAF was in place to protect public-facing web applications from outside threats.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the WAF configurations for the production server to determine that a WAF was in place to protect public-facing web applications from outside threats.	No exceptions noted.
		Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.	Inspected the company's website, compliance automation software, code of conduct, internal communication channel and incident management and escalation policies and procedures to determine that internal communication channels were in place for employees to report failures, events, incidents, concerns, and other issues to company management.	No exceptions noted.
		An IDS is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected.	Inspected the network diagram and IDS configurations to determine that an IDS was in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and was configured to alert personnel when a potential intrusion was detected.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not Applicable.	Not Applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The Company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan is reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	Inspected the incident response policies and procedures, including the revision history, to determine that the Company had a documented incident response plan that outlined roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents, and the incident response plan was reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	No exceptions noted.
		The Company evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	Inquired of the VP, Security and IT Operations, regarding security incidents to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	Testing of the control activity disclosed that no incidents occurred during the review period.
		The Company has identified and documented roles and responsibilities for incident management.	Inspected the incident response policies and procedures to determine that the Company had identified and documented roles and responsibilities for incident management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs.	Inquired of the VP, Security and IT Operations regarding customer support issues to determine that the company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the incident management and escalation policies and procedures to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the entity's website to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting ticket for a sample of customer support issues to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	Testing of the control activity disclosed that there were no customer support issues reported during the review period.
		Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.	Inspected the company's website, compliance automation software, code of conduct, internal communication channel and incident management and escalation policies and procedures to determine that internal communication channels were in place for employees to report failures, events, incidents, concerns, and other issues to company management.	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 Company provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	Inquired of the VP, Security and IT Operations, regarding breach notifications to determine that the Company provided communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that the Company provided communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incidents to determine that the Company provided communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.	Testing of the control activity disclosed that no critical security incidents and breaches occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan is reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	Inspected the incident response policies and procedures, including the revision history, to determine that the Company had a documented incident response plan that outlined roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents, and the incident response plan was reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	No exceptions noted.
		The Company evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	Inquired of the VP, Security and IT Operations, regarding security incidents to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that the Company evaluated security events to determine if they constituted an incident, and incidents were assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.	Testing of the control activity disclosed that no incidents occurred during the review period.
		The Company has identified and documented roles and responsibilities for incident management.	Inspected the incident response policies and procedures to determine that the Company had identified and documented roles and responsibilities for incident management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company provides external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs.	Inquired of the VP, Security and IT Operations regarding customer support issues to determine that the company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the incident management and escalation policies and procedures to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.
			Inspected the entity's website to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting ticket for a sample of customer support issues to determine that the Company provided external communication mechanisms for customers and third-parties to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. and customer communications were responded to within defined SLAs.	Testing of the control activity disclosed that there were no customer support issues reported during the review period.
		Internal communication channels are in place for employees to report failures, events, incidents, concerns, and other issues to company management.	Inspected the company's website, compliance automation software, code of conduct, internal communication channel and incident management and escalation policies and procedures to determine that internal communication channels were in place for employees to report failures, events, incidents, concerns, and other issues to company management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The Company has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan is reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	Inspected the incident response policies and procedures, including the revision history, to determine that the Company had a documented incident response plan that outlined roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents, and the incident response plan was reviewed at least annually and updated as needed according to lessons learned from previous incidents and industry developments.	No exceptions noted.
		The Company has a defined Business Continuity Plan that outlines strategies for maintaining operations during a disruption.	Inspected the business continuity plans to determine that the Company had a defined Business Continuity Plan that outlined strategies for maintaining operations during a disruption.	No exceptions noted.
		The Company has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	Inspected the disaster recovery plans to determine that the Company had a documented disaster recovery plan that outlined roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company conducts tests of the business continuity and disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary.	Inspected the completed business continuity and disaster recovery test results to determine that the Company conducted tests of the business continuity and disaster recovery plans at least annually, the results and lessons learned were documented, and updates to the plans were made as necessary.	No exceptions noted.
		The Company has identified and documented roles and responsibilities for incident management.	Inspected the incident response policies and procedures to determine that the Company had identified and documented roles and responsibilities for incident management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Changes to system components in the production environment are made according to established procedures that include documentation and testing.	Inspected the change management policies and procedures to determine that changes to system components in the production environment were made according to established procedures that included documentation and testing.	No exceptions noted.
			Inspected the supporting change ticket for a sample of system and infrastructure changes to determine that changes to system components in the production environment were made according to established procedures that included documentation and testing.	No exceptions noted.
		The Company uses a version control system to manage source code, change documentation and tracking, release labeling, and other change management tasks.	Inspected the source code repository configurations to determine that the Company used a version control system to manage source code, change documentation and tracking, release labeling, and other change management tasks.	No exceptions noted.
		The company has enabled change-detection mechanism to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data cannot be changed without generating alerts.	Inspected the source code repository configurations to determine that the company had enabled change-detection mechanism to detect unauthorized modification of critical system files, configuration files, audit files, or content files to ensure critical data could not be changed without generating alerts.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The company has a documented a policy that describes the requirements for managing changes across the organization, including changes to infrastructure, systems, and applications.	Inspected the change management policies and procedures to determine that the company had a documented a policy that described the requirements for managing changes across the organization, including changes to infrastructure, systems, and applications.	No exceptions noted.
		Access to make changes in production environments is restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures.	Inquired of the VP, Security and IT Operations regarding the ability to migrate changes into the production environment to determine that access to make changes in production environments was restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures.	No exceptions noted.
			Inspected the list of users with the ability to deploy changes into the production environment to determine that access to make changes in production environments was restricted to authorized personnel in accordance with segregation of duties principles and the company's documented policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Pre-production environments are separated from production environments and the separation is enforced with access controls.	Inspected the separate development and production environments to determine that pre-production environments were separated from production environments and the separation was enforced with access controls.	No exceptions noted.
		The Company communicates system changes via release notes or change log via periodic communications.	Inspected the internal communication channel and the supporting e-mail communications to external users to determine that the Company communicated system changes via release notes or change log via periodic communications.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The Company has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	Inspected the risk assessment policies and procedures to determine that the Company had defined and documented a process for risk assessment and risk management that outlined the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria.	No exceptions noted.
		The Company maintains cybersecurity insurance to mitigate the financial impact of security incidents and business disruptions.	Inspected the cybersecurity insurance documentation to determine that the Company maintained cybersecurity insurance to mitigate the financial impact of security incidents and business disruptions.	No exceptions noted.
		The Company conducts risks assessments annually as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented.	Inspected the completed risk assessment to determine that the Company conducted risks assessments annually as required by company policy and compliance requirements, the risk assessment included consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk, a risk owner was assigned to each risk, every risk was assigned a risk treatment option, and the results of the risk assessment were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle.	Inspected the vendor management policies and procedures to determine that the Company had a documented policy that outlined requirements for managing vendor and third-party relationships through their entire life cycle.	No exceptions noted.
		Management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.	Inspected the completed risk assessment to determine that management had documented a risk treatment plan to formally manage risks identified in risk assessment activities.	No exceptions noted.
		The Company performs due diligence activities prior to engaging with a new service provider or vendor. Results of the due diligence activities including action items are documented.	Inspected the vendor listing and completed supplier evaluation form for a sample of third-parties to determine that the Company performed due diligence activities prior to engaging with a new service provider or vendor, and the results of the due diligence activities including action items were documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company maintains a third-party register that includes a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc. The Company executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider.	Inspected the third-party register to determine that the Company maintained a third-party register that included a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc., and the Company executed agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outlined the responsibilities of each vendor or service provider.	No exceptions noted.
			Inspected the third-party agreement for a sample of third-parties to determine that the Company maintained a third-party register that included a complete and accurate list of third-parties, relationship owners, description for each of the services provided, risk ratings, results of third-party risk management activities, etc., and the Company executed agreements with third-party and service providers involved in accessing, processing, storing or managing information assets that outlined the responsibilities of each third-party and service provider.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, are documented.	Inspected the compliance reports and associated security review documentation for a sample of third-parties to determine that the Company obtained and reviewed compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third-parties' compliance with industry frameworks, regulations, standards and the Company's requirements, and the results of the review and action items, if any, were documented.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
CC1.1 CC1.4	Background checks are conducted on eligible personnel prior to hire as permitted by local laws.	Inspected the completed background check for a sample of new hires to determine that background checks were conducted on eligible personnel prior to hire as permitted by local laws.	Testing of the control activity disclosed that background check was not completed in a timely manner for one of one new hire sampled.	This is noted by the Glooko team and has been addressed since the end of the review period.