OpenSesame Inc.
Type 2 SOC 2
2021

REPORT ON OPENSESAME 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

January 1, 2021 to September 30, 2021

Table of Contents

SECTION 1

ASSERTION OF OPENSESAME INC. MANAGEMENT

ASSERTION OF OPENSESAME INC. MANAGEMENT

November 12, 2021

We have prepared the accompanying description of OpenSesame Inc.'s ('OpenSesame' or 'the Company') eLearning SaaS Services System titled "OpenSesame Inc.'s Description of Its eLearning SaaS Services System throughout the period January 1, 2021 to September 30, 2021" (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 eLearning SaaS Services System that may be useful when assessing the risks arising from interactions with OpenSesame's system, particularly information about system controls that OpenSesame 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*).

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

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

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

a. the description presents OpenSesame's eLearning SaaS Services System that was designed and implemented throughout the period January 1, 2021 to September 30, 2021, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that OpenSesame'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 OpenSesame's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that OpenSesame'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 OpenSesame's controls operated effectively throughout that period.

Joshua Blank
President & Chief Product Officer
OpenSesame Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: OpenSesame Inc.

Scope

We have examined OpenSesame's accompanying description of its eLearning SaaS Services System titled "OpenSesame Inc.'s Description of Its eLearning SaaS Services System throughout the period January 1, 2021 to September 30, 2021" (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 January 1, 2021 to September 30, 2021, to provide reasonable assurance that OpenSesame'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*).

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

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

Service Organization's Responsibilities

OpenSesame 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 OpenSesame's service commitments and system requirements were achieved. OpenSesame has provided the accompanying assertion titled "Assertion of OpenSesame Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. OpenSesame 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.

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 OpenSesame’s eLearning SaaS Services System that was designed and implemented throughout the period January 1, 2021 to September 30, 2021, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that OpenSesame’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 OpenSesame’s controls throughout that period.
c. the controls stated in the description operated effectively throughout the period January 1, 2021 to September 30, 2021, to provide reasonable assurance that OpenSesame’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 OpenSesame’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 OpenSesame, user entities of OpenSesame’s eLearning SaaS Services System during some or all of the period January 1, 2021 to September 30, 2021, business partners of OpenSesame subject to risks arising from interactions with the eLearning SaaS Services System, 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
November 12, 2021

SECTION 3

OPENSESAME INC.’S DESCRIPTION OF ITS ELEARNING SAAS SERVICES SYSTEM THROUGHOUT THE PERIOD JANUARY 1, 2021 TO SEPTEMBER 30, 2021

OVERVIEW OF OPERATIONS

Company Background

OpenSesame was founded in 2011 to provide a better model for distributing standards-based online training. OpenSesame's main office is located in Portland, Oregon, with a European division in London.

OpenSesame's Software as a Service (SaaS) platform allows publishers of eLearning content to sell products through a secure, centrally managed system.

OpenSesame's technology allows delivery of content on the platform to any standards compliant Learning Management System (LMS) or Learning eXperience Platform (LXP). In addition, for customers who do not have a suitable platform, OpenSesame offers "Course Cloud," a system allowing students to launch content from their e-mail.

OpenSesame serves major industries and is focused on large enterprises in the Global 2000. OpenSesame's recommendation algorithms and Curation Alignment Process (CAP) provide customers with automated, targeted recommendations based upon their industry, size, location, and activity within the platform.

OpenSesame operates as a marketplace and does not produce content itself. Rather, OpenSesame partners with content publishers from around the world and employs strict, industry-leading quality standards for inclusion in the marketplace.

Description of Services Provided

OpenSesame provides eLearning market participants a platform to conduct commerce as well as discover, curate, and consume content via these services:

- Content management system and ingestion pipeline:
    - Publishers upload and merchandise content to appear in the marketplace
    - OpenSesame processes content to allow it to be delivered and managed on the platform
- Content player:
    - Students launch standards-compliant content
    - OpenSesame delivers results (completion, score, etc.) to customer's Learning Management System
- Catalog:
    - Customers can browse and purchase from OpenSesame's catalog of 20,000+ curated eLearning courses
    - The OpenSesame Plus subscription offers unlimited access to 10,000+ titles from the most trusted publishers
- Insights:
    - Surfaces usage, activity, and ratings trends
- Recommender:
    - Based upon a customer's usage of the system and company profile, OpenSesame's recommendation systems assist customers in creating training programs covering any business topic or job title
- Course Cloud:
    - For customers who do not have an LMS, customers can utilize Course Cloud to invite their students to take courses through an e-mail link

Principal Service Commitments and System Requirements

OpenSesame designs, operates, and supports its platform to meet specific commitments to its customers and community.

Service commitments such as uptime and ticket response are maintained and tracked via internal Service Level Objectives (SLOs) and communicated to customers through Service Level Agreements (SLAs).

Security, Privacy, and Legal commitments pertaining to relevant legislation and customers' standards of compliance are documented and communicated to internal staff and customers through training, policy documentation, and SLAs. OpenSesame's platform is designed to secure customer data and ensure compliance with legal requirements through a standardized set of technical and organizational measures including, but not limited to:

- The use of industry-standard network security firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Data Loss Prevention (DLP), and antivirus
- Pre-employment background and drug screening
- Annual required security training for staff
- Rigorous change control process
- Encryption of customer data in transit and at rest

OpenSesame establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in OpenSesame's system policies and procedures, system design documentation, and contracts with customers. Information security policies 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 platform.

Components of the System

Infrastructure and Software

Primary Infrastructure and Software used to provide OpenSesame's eLearning SaaS Services System includes the following:

Primary Infrastructure and Software		
Hardware	**Type**	**Purpose**
Web Application Firewall (WAF)	Signal Sciences	Protect infrastructure from attacks, limit exposed ports
Content Delivery Network (CDN)	Fastly	Accelerates web traffic through caching
IDS and File Integrity Monitoring (FIM)	Threat Stack	Detects and alarms on attacks; audits infrastructure for rule exceptions
IDS	AWS GuardDuty	Threat Detection Service
Antivirus	Sophos	Prevents known viruses and malware
DLP	Sophos	Stops data exfiltration attempts
Identity and Access Management (IAM)	Okta	Controls access to Okta integrated resources via Single Sign-On (SSO)
Platform as a Service (PaaS)	AWS	Provides basic infrastructure for delivering the services
AWS Service	AWS Simple Storage Service (AWS S3)	Object storage service

Primary Infrastructure and Software		
Hardware	**Type**	**Purpose**
AWS Service	AWS Key Management Service (KMS)	Key management
Relational Database Service (RDS)	AWS RDS MySQL	Database
Infrastructure as a Service (IaaS)	GCP	Backup services as a failsafe against catastrophic failure within AWS
Platform	OpenSesame	Platform (Catalog and Player) supporting the eLearning SaaS Services System
Governance, Risk Management, and Compliance (GRC)	ZenGRC	GRC tool utilized to oversee, manage, and evaluate risks internally and with third parties
Mobile Device Management (MDM)	Jamf	Manages employee mobile devices
Vulnerability Scanning	WhiteHat	Application security platform utilized in identifying vulnerabilities

People

OpenSesame employs a staff of approximately 180 employees organized into these functional areas:

- Community Support staff field incoming technical support requests and general inquiries from customers and are organized into three tiers:
  - Tier 1: incoming chat and e-mail inquiries
  - Tier 2: cases requiring escalation to a technical resource
  - Tier 3: cases requiring advanced technical expertise or investigation
- Sales and Customer Success staff are assigned to customers and partners during onboarding and are the main account contact for customers and partners regarding contracting, usage, implementation, and curation requests
- Partner team maintains industry partnerships and generates sales leads in cooperation with the partners
- Curation staff manage content publishers and curate content:
  - Business development and relationship management for the publisher community
  - Curation on behalf of individual customers and the marketplace as a whole
  - Quality control
- Product Development and Operations build, deploy, and support the platform, as well as maintain the Quality Assurance (QA) and change management processes
- Business Intelligence staff maintain internally facing applications and data supporting company-wide business functions
- Marketing staff collaborate with Sales and Partner teams to generate awareness and leads
- Finance team is responsible for financial planning, budgeting, cash management, collections, and AP/AR
- People team is responsible for employee training programs, employee wellbeing, onboarding, and general HR functions
- Information Technology (IT) staff support OpenSesame’s user population through helpdesk and technical onboarding and own security posture and training. IT administers internally facing applications and is responsible for user population audits and offboarding
- Security staff supports teams in protecting company assets and customer data

Data

Data imported, processed, and generated by the OpenSesame platform consists of:

- Customer data:
    - Company/contracting data
    - Company contact data
    - Student data
- Content data:
    - Content assets
    - Content metadata

Customers provide data during contracting that enables OpenSesame to service their account. This includes account contact, billing contact, and company address.

When students launch courses, OpenSesame receives the Student's Name and Student ID from the customer's LMS in an automated process defined by publicly available learning interoperability standards such as Experience Application and Programming Interface (xAPI), Shareable Content Object Reference Model (SCORM), Learning Tools Interoperability (LTI), and Aviation Industry Computer Based Training Committee (AICC). Privacy controls within the platform enable customers to optionally anonymize or discard this data if their compliance posture does not allow such data to be shared with third parties. If a customer is using Course Cloud, the student's e-mail address acts as their Student ID.

OpenSesame's Reporting and Insights systems make licensing and activity information available to customers on-demand via web portal and Comma-Separated Values (CSV) download. OpenSesame's access to customer reports and data is limited based upon job role and account assignment.

Data exchange is protected by Transport Layer Security (TLS) 1.2 or greater.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to the OpenSesame policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any OpenSesame team member.

Physical Security

OpenSesame utilizes AWS to process customer data and deliver the in-scope services. See https://aws.amazon.com/compliance/ for physical security and compliance information on their facilities.

OpenSesame utilizes GCP as a failsafe backup in case of catastrophic failure of AWS. See https://cloud.google.com/security/compliance for physical security and compliance information on their facilities.

Refer to the 'Subservice Organizations' section below for controls managed by the subservice organizations.

Logical Access

OpenSesame utilizes role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists.

Employees and contractors access the OpenSesame platform application using their Okta username, password, and Multi-Factor Authentication (MFA) device. Employee workstations are configured according to security policies including automatic screen lock after inactivity. Employees and contractors may access the platform application from the OpenSesame office or by connecting to the Virtual Private Network (VPN). VPN users are authenticated via Security Assertion Markup Language (SAML) through the identity provider, Okta.

Customer employees access the OpenSesame platform application using their e-mail address and password. Passwords must meet password policy requirements.

Access to the OpenSesame platform is secured with TLS 1.2+.

OpenSesame's IT team manages access to the platform application through onboarding, offboarding, and job change tickets generated by the People team. Roles are predefined and assigned according to job function. Terminated employees' access is revoked concurrently with notification of termination.

Computer Operations - Backups

Customer data is stored in an online RDBMS (Relational Database Management System) within AWS with replication spanning multiple datacenters and geographic regions. The AWS RDS cluster is configured to retain eight days of backups which are available for immediate restore to any point in time.

An additional daily failsafe backup is stored in Amazon S3 and also shipped to GCP in case of catastrophic failure of multiple AWS services, availability zones, and regions.

Refer to the 'Subservice Organizations' section below for additional controls managed by the subservice organizations.

Computer Operations - Availability

OpenSesame's infrastructure is hosted in AWS and is not dependent upon any single point of failure. Networks, servers, databases, and other services are either load-balanced between multiple AZs (Availability Zones, which are groups of datacenters within a Region) or have a hot standby in a second AZ. For more information on AWS AZs and Regions, please see https://aws.amazon.com/compliance.

Activity and usage alarms are configured to proactively monitor system resources and activity. Automated monitoring of resources drives both auto-scaling in case of increased load and self-healing via launching of new instances in case of server failure. Non-autoscaling resources are monitored continuously to ensure sufficient capacity is available.

Automated load testing is performed regularly to ensure that the platform can scale to meet load projections.

Refer to the 'Subservice Organizations' section below for additional controls managed by the subservice organizations.

Change Control

OpenSesame maintains a documented Change Management Policy to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, QA testing requirements, and required approval procedures.

System changes are documented in a ticket and pull request (PR) and tracked through the change process to implementation. Manual test results are documented and maintained with the associated ticket and/or PR. System changes are tested through a continuous integration (CI)/continuous delivery (CD) pipeline that runs automated tests and security checks prior to deployment. Development and testing are performed in an environment that is logically separated from the production environment. Peer reviews are performed on changes prior to migration to the production environment, which are documented within the ticketing system.

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.

OpenSesame has implemented a patch management process to ensure that infrastructure systems are patched in accordance with vendor recommended operating system patches. OpenSesame system owners review proposed operating system patches to determine whether the patches are applied. OpenSesame Engineering, IT, and Security teams are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. OpenSesame staff validate that patches have been installed and, if applicable, that required reboots or other activation steps have been successfully completed.

Data Communications

The OpenSesame platform is secured through defense in depth, utilizing multiple layers of network security to protect information flowing to and from the platform.

A WAF offers Distributed Denial of Service (DDOS) and application security outside the perimeter of OpenSesame’s infrastructure. Only Hypertext Transfer Protocol Secure (HTTPS) traffic secured by TLS 1.2 or greater may transit the WAF, which blocks traffic from known compromised Internet Protocol (IP) addresses and inspects the payload of every incoming request.

Within AWS, an additional WAF and Virtual Private Cloud (VPC) network configuration provide further protection against malicious network activity.

Finally, a host-based IDS and DLP is configured on every production instance to provide protection against persistent threats and data exfiltration attempts. A 24/7/365 Security Operations Center is contracted to examine and respond to critical alerts.

A continuous vulnerability scan is conducted against the platform. The scanner is allow-listed to prevent the network security services from blocking its traffic, ensuring that OpenSesame’s native configuration is subject to the scanner.

An annual network penetration test and an additional application business logic test are performed by third parties.

Any critical, high, or medium severity vulnerabilities detected and classified by the scanner or penetration/business logic test are triaged immediately upon receipt of alert, and if determined to be valid and of critical or high risk, remediated immediately with a target deployment time of under 24 hours.

Refer to the ‘Subservice Organizations’ section below for additional controls managed by the subservice organizations.

Boundaries of the System

The scope of this report includes the eLearning SaaS Services System performed in the Portland, Oregon facility.

This report does not include the cloud hosting services provided by AWS in US-West-1 and US-West-2 and the cloud storage services provided by GCP in US-West-1.

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

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of OpenSesame's control environment, affecting the design, administration, and monitoring of other components.

Integrity and ethical behavior are the product of OpenSesame's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of shared values and behavioral standards to personnel through policy statements, codes of conduct, company standards, and by example by senior leadership and managers.

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

- Core values are communicated from executive management to personnel through policies, procedures, and the employee handbook
- The employee handbook communicates workforce conduct standards and enforcement procedures, which include disciplinary actions, up to and including termination as potential sanctions for employee misconduct or violations
- Personnel are required to undergo a background check provided by a third-party screening company, upon hire
- Personnel are required to acknowledge the employee handbook upon hire and annually thereafter
- An anonymous hotline is in place to allow employees, third parties, and customers to report unethical behavior in a confidential and anonymous manner

Commitment to Competence

OpenSesame management defines competence as the knowledge and skills necessary to accomplish tasks defined by employees' job descriptions. Management's commitment to competence includes management's 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 are described below:

- Hiring Managers and the Hiring team are responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives
- The entity has established formal hiring practices to support the hiring of personnel with the qualifications and skills necessary to support the system. As part of the hiring process, the entity evaluates the competency, qualifications, and experience of candidates for hire by reviewing resumes, validating qualifications against the job description, and conducting interviews

- The entity maintains an organizational chart and job descriptions for personnel, including executive management, to delineate reporting lines and other related responsibilities. The organizational chart and job descriptions are reviewed periodically throughout the year, but no less than annually, and made available to personnel to enable awareness of their responsibilities
- Performance management procedures are documented to give guidance to personnel on the overall continuous performance management process
- The entity employs the progressive discipline approach, which includes individual coaching and a Performance Improvement Plan (PIP), for any personnel failing to meet entity standards for work performance
- The entity utilizes a continuous performance management approach for personnel to assess their performance and provide feedback via various meetings throughout the year, but no less than annually
- The entity provides various training programs, including continuing education and security awareness training, through a Learning Management System (LMS) to ensure skill sets and technical competency of personnel are developed and maintained
- Changes or updates to the overall training programs delivered to personnel are assessed at least annually by management
- Personnel are required to complete security awareness training upon hire and annually thereafter
- The entity evaluates the competencies and experience of third-party vendors prior to working with them

Management's Philosophy and Operating Style

OpenSesame's management philosophy and operating style encompass a broad range of characteristics, including 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 are described below:

- The entity establishes objectives that are reflective of management's choices about growth, innovation, entity structure, the industry, and performance of the entity
- The Board of Directors meet with senior management quarterly to provide overall governance support to the entity
- The Leadership team meets weekly to review and discuss financial metrics, entity performance, resources, and business plans to ensure alignment with the corporate goals and objectives
- The Security team meets on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed

Organizational Structure and Assignment of Authority and Responsibility

OpenSesame'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 these needs. This organizational structure is based, in part, on its size and the nature of its activities.

OpenSesame'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.

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

- The entity maintains an organizational chart and job descriptions for personnel, including executive management, to delineate reporting lines and other related responsibilities. The organizational chart and job descriptions are reviewed periodically throughout the year, but no less than annually, and made available to personnel to enable awareness of their responsibilities
- The entity has documented policies and procedures in support of the internal controls and objectives, which communicate control responsibilities and define system boundaries to personnel and are made available through the entity's intranet site

Human Resources Policies and Practices

OpenSesame'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, ensuring that the service organization is operating at maximum efficiency. OpenSesame'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 are described below:

- Hiring Managers and the Hiring team are responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives
- The entity has established formal hiring practices to support the hiring of personnel with the qualifications and skills necessary to support the system. As part of the hiring process, the entity evaluates the competency, qualifications, and experience of candidates for hire by reviewing resumes, validating qualifications against the job description, and conducting interviews
- The entity employs the progressive discipline approach, which includes individual coaching and a PIP, for any personnel failing to meet entity standards for work performance
- The entity utilizes a continuous performance management approach for personnel to assess their performance and provide feedback via various meetings throughout the year, but no less than annually
- The entity provides various training programs, including continuing education and security awareness training, through a LMS to ensure skill sets and technical competency of personnel are developed and maintained

Risk Assessment Process

OpenSesame's risk assessment process identifies and manages risks that could potentially affect OpenSesame's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. OpenSesame identifies the underlying sources of risk, measures the impact to the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by OpenSesame, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

OpenSesame attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with senior management.

The entity utilizes a GRC tool to manage internal risk and compliance activities and risks associated with external parties. At least annually, personnel with risk management responsibilities assess changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives in the GRC tool.

Integration with Risk Assessment

The complex environment in which OpenSesame operates; the commitments, agreements, and responsibilities of OpenSesame's eLearning SaaS Services System; as well as the nature of the components of the system may result in risks that the criteria will not be met. OpenSesame 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, OpenSesame'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 are an integral component of OpenSesame'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 OpenSesame, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, partners, and employees.

Various weekly 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 to provide staff with input and updates on issues affecting the organization and its employees. Senior executives lead the meetings with information gathered from employees. General updates to entity-wide security policies and procedures are communicated to the appropriate OpenSesame personnel in meetings, via e-mail messages, and via eLearning delivered through OpenSesame's internal learning management system.

Specific information systems used to support OpenSesame's eLearning SaaS Services System are described in the 'Description of Services' section above.

Monitoring Controls

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

On-Going Monitoring

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

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

Reporting Deficiencies

A GRC tool and ticketing system is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. The Security team meets on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization’s last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization’s last review.

Criteria Not Applicable to the System

All Common/Security criterion was applicable to the OpenSesame eLearning SaaS Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS in US-West-1 and US-West-2 and the cloud storage services provided by GCP in US-West-1.

Subservice Description of Services

AWS provides PaaS services utilized to deliver OpenSesame’s services, including compute, storage, high-availability, backup, and security.

GCP provides backup services as a failsafe against catastrophic failure within AWS.

Complementary Subservice Organization Controls

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

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	CC6.1, CC6.4	KMS-Specific - Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
	CC6.1, CC6.6	S3-Specific - Network devices are configured by AWS to only allow access to specific ports on other server systems within Amazon S3.
		S3-Specific - External data access is logged with the following information: data accessor IP address, object and operation. Logs are retained for at least 90 days.
		S3-Specific - S3 generates and stores a one-way salted HMAC of the customer encryption key. This salted HMAC value is not logged.
		KMS-Specific - Requests in KMS are logged in AWS CloudTrail.
	CC6.1, CC6.6, CC6.7	KMS-Specific - Customer master keys used for cryptographic operations in KMS are logically secured so that no single AWS employee can gain access to the key material.
		KMS-Specific - AWS Services that integrate with AWS KMS for key management use a 256-bit data key locally to protect customer content.
		KMS-Specific - The key provided by KMS to integrated services is a 256-bit key and is encrypted with a 256-bit advanced encryption standard (AES) master key unique to the customer’s AWS account.
	CC6.4	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.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Access to server locations is managed by electronic access control devices.
	CC6.4, CC7.2	Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
	CC6.5	All AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.
		AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.
		AWS retains customer content per customer agreements.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
	CC7.2	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
	CC7.3, CC7.4, CC7.5	AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.

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

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.1	GCP is configured to log various metrics and events such as administrator and data access events.
		Customer data that is uploaded or created is encrypted at rest.
	CC6.4	Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, biometric identification mechanisms, and/or physical locks.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high-security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
	CC6.4, CC7.2	Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.
	CC6.5	The organization sanitizes storage media prior to disposal, release from organizational control, or release for reuse.

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

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

COMPLEMENTARY USER ENTITY CONTROLS

OpenSesame'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 OpenSesame's services to be solely achieved by OpenSesame control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of OpenSesame'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 OpenSesame.
2. User entities are responsible for notifying OpenSesame 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 OpenSesame 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 OpenSesame services.
6. User entities are responsible for providing OpenSesame with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying OpenSesame 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 managing their users, accounts, and passwords.

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 OpenSesame's description of the system. Any applicable trust services criteria that are not addressed by control activities at OpenSesame 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 OpenSesame was limited to the Trust Services Criteria, related criteria and control activities specified by the management of OpenSesame and did not encompass all aspects of OpenSesame'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 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.	Core values are communicated from executive management to personnel through policies, procedures, and the employee handbook.	Inspected the entity's policies and procedures, the employee handbook, and the entity's intranet site to determine that core values were communicated from executive management to personnel through policies, procedures, and the employee handbook.	No exceptions noted.
		The employee handbook communicates workforce conduct standards and enforcement procedures, which include disciplinary actions, up to and including termination as potential sanctions for employee misconduct or violations.	Inspected the employee handbook to determine that the employee handbook communicated workforce conduct standards and enforcement procedures, which included disciplinary actions, up to and including termination as potential sanctions for employee misconduct or violations.	No exceptions noted.
		The employee handbook is reviewed for accuracy at least annually and updated accordingly.	Inspected the employee handbook including the review date to determine that the employee handbook was reviewed for accuracy at least annually and updated accordingly.	No exceptions noted.
		Personnel are required to undergo a background check provided by a third-party screening company, upon hire.	Inquired of the Security Analyst regarding the hiring process to determine that personnel were required to undergo a background check provided by a third-party screening company, upon hire.	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 recruitment process procedures to determine that personnel were required to undergo a background check provided by a third-party screening company, upon hire.	No exceptions noted.
			Inspected the completed background check report for a sample of new hires to determine that personnel were required to undergo a background check provided by a third-party screening company, upon hire.	No exceptions noted.
			Inspected the completed background check report for the population of contractors with system access to determine that personnel were required to undergo a background check provided by a third-party screening company, upon hire.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook upon hire and annually thereafter.	Inquired of the Security Analyst regarding the hiring process to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	No exceptions noted.
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	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 completed employee handbook acknowledgement log for a sample of new hires to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	No exceptions noted.
			Inspected the completed employee handbook acknowledgement log for a sample of current employees to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	No exceptions noted.
		The entity utilizes a continuous performance management approach for personnel to assess their performance and provide feedback via various meetings throughout the year, but no less than annually.	Inquired of the Security Analyst regarding performance management to determine that the entity utilized a continuous performance management approach for personnel to assess their performance and provided feedback via various meetings throughout the year, but no less than annually.	No exceptions noted.
			Inspected the performance management procedures to determine that the entity utilized a continuous performance management approach for personnel to assess their performance and provided feedback via various meetings throughout the year, but no less than annually.	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 completed performance management documentation for a sample of current employees to determine that the entity utilized a continuous performance management approach for personnel to assess their performance and provided feedback via various meetings throughout the year, but no less than annually.	No exceptions noted.
		An anonymous hotline is in place to allow employees, third parties, and customers to report unethical behavior in a confidential and anonymous manner.	Inquired of the Security Analyst regarding unethical behavior to determine that an anonymous hotline was in place to allow employees, third parties, and customers to report unethical behavior in a confidential and anonymous manner.	No exceptions noted.
			Inspected the employee handbook and the terms and conditions page on the entity's externally-facing website to determine that an anonymous hotline was in place to allow employees, third parties, and customers to report unethical behavior in a confidential and anonymous manner.	No exceptions noted.
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 Board of Directors includes senior management and advisors who are independent from management.	Inspected the Board of Directors members listing to determine that the Board of Directors included senior management and advisors who were independent from 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**
		Bylaws are in place that outline the Board of Directors' structure and responsibilities of its members.	Inspected the bylaws for the Board of Directors and any associated addendums to determine that bylaws were in place that outlined the Board of Directors' structure and responsibilities of its members.	No exceptions noted.
		The Board of Directors meet with senior management quarterly to provide overall governance support to the entity.	Inspected the Board of Directors meeting minutes for a sample of quarters to determine that the Board of Directors met with senior management quarterly to provide overall governance support to the entity.	No exceptions noted.
		The Leadership team meets weekly to review and discuss financial metrics, entity performance, resources, and business plans to ensure alignment with the corporate goals and objectives.	Inspected the weekly Leadership team recurring meeting invite, running meeting agenda, and meeting minutes for the entire review period to determine that the Leadership Team met weekly to review and discuss financial metrics, entity performance, resources, and business plans to ensure alignment with the corporate goals and objectives.	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 entity maintains an organizational chart and job descriptions for personnel, including executive management, to delineate reporting lines and other related responsibilities. The organizational chart and job descriptions are reviewed periodically throughout the year, but no less than annually, and made available to personnel to enable awareness of their responsibilities.	Inspected the organizational chart, including revision history, job description for the population of job roles, including date of last review, and the entity's intranet site to determine that the entity maintained an organizational chart and job descriptions for personnel, including executive management, to delineate reporting lines and other related responsibilities, and that the organizational chart and job descriptions were reviewed periodically throughout the year, but no less than annually, and made available to personnel to enable awareness of their responsibilities.	No exceptions noted.
		The entity utilizes a continuous performance management approach to assess the performance of executive management and provide feedback via various meetings throughout the year, but no less than annually.	Inquired of the Security Analyst regarding executive management to determine that the entity utilized a continuous performance management approach to assess the performance of executive management and provided feedback via various meetings throughout the year, but no less than annually.	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 performance management procedures to determine that the entity utilized a continuous performance management approach to assess the performance of executive management and provided feedback via various meetings throughout the year, but no less than annually.	No exceptions noted.
			Inspected the completed performance management documentation for a sample of executive management members to determine that the entity utilized a continuous performance management approach to assess the performance of executive management and provided feedback via various meetings throughout the year, but no less than annually.	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.	The Board of Directors meet with senior management quarterly to provide overall governance support to the entity.	Inspected the Board of Directors meeting minutes for a sample of quarters to determine that the Board of Directors met with senior management quarterly to provide overall governance support to the entity.	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 entity maintains an organizational chart and job descriptions for personnel, including executive management, to delineate reporting lines and other related responsibilities. The organizational chart and job descriptions are reviewed periodically throughout the year, but no less than annually, and made available to personnel to enable awareness of their responsibilities.	Inspected the organizational chart, including revision history, job description for the population of job roles, including date of last review, and the entity's intranet site to determine that the entity maintained an organizational chart and job descriptions for personnel, including executive management, to delineate reporting lines and other related responsibilities, and that the organizational chart and job descriptions were reviewed periodically throughout the year, but no less than annually, and made available to personnel to enable awareness of their responsibilities.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook upon hire and annually thereafter.	Inquired of the Security Analyst regarding the hiring process to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	No exceptions noted.
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	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 completed employee handbook acknowledgement log for a sample of new hires to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	No exceptions noted.
			Inspected the completed employee handbook acknowledgement log for a sample of current employees to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	No exceptions noted.
		Management performs annual due diligence procedures on third-party vendors who are classified as a sub-processor. Monitoring procedures include maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	Inquired of the Security Analyst regarding the third-party vendor risk assessment process to determine that management performed annual due diligence procedures on third-party vendors who were classified as a sub-processor, and that monitoring procedures included maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	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 vendor risk management policy to determine that management performed annual due diligence procedures on third-party vendors who were classified as a sub-processor, and that monitoring procedures included maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	No exceptions noted.
			Inspected the listing of third-party sub-processors, attestation report, and vendor attestation report review meeting minutes for a sample of third-party vendors to determine that management performed annual due diligence procedures on third-party vendors who were classified as a sub-processor, and that monitoring procedures included maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Hiring Managers and the Hiring team are responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives.	Inspected the recruitment process procedures, engineering hiring process procedures, and the careers page on the entity’s externally-facing website to determine that Hiring Managers and the Hiring team were responsible for attracting individuals with competencies and experience that aligned with the entity's goals and objectives.	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 entity has established formal hiring practices to support the hiring of personnel with the qualifications and skills necessary to support the system. As part of the hiring process, the entity evaluates the competency, qualifications, and experience of candidates for hire by reviewing resumes, validating qualifications against the job description, and conducting interviews.	Inquired of the Security Analyst regarding the hiring process to determine that the entity had established formal hiring practices to support the hiring of personnel with the qualifications and skills necessary to support the system, and that as part of the hiring process, the entity evaluated the competency, qualifications, and experience of candidates for hire by reviewing resumes, validating qualifications against the job description, and conducting interviews.	No exceptions noted.
			Inspected the recruitment process procedures, engineering hiring process procedures, and the careers page on the entity's external-facing website to determine that the entity had established formal hiring practices to support the hiring of personnel with the qualifications and skills necessary to support the system, and that as part of the hiring process, the entity evaluated the competency, qualifications, and experience of candidates for hire by reviewing resumes, validating qualifications against the job description, and conducting interviews.	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 job description for the population of job roles and the candidate interview feedback and scorecards for a sample of new hires to determine that the entity had established formal hiring practices to support the hiring of personnel with the qualifications and skills necessary to support the system, and that as part of the hiring process, the entity evaluated the competency, qualifications, and experience of candidates for hire by reviewing resumes, validating qualifications against the job description, and conducting interviews.	No exceptions noted.
		Personnel are required to undergo a background check provided by a third-party screening company, upon hire.	Inquired of the Security Analyst regarding the hiring process to determine that personnel were required to undergo a background check provided by a third-party screening company, upon hire.	No exceptions noted.
			Inspected the recruitment process procedures to determine that personnel were required to undergo a background check provided by a third-party screening company, upon hire.	No exceptions noted.
			Inspected the completed background check report for a sample of new hires to determine that personnel were required to undergo a background check provided by a third-party screening company, upon hire.	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 completed background check report for the population of contractors with system access to determine that personnel were required to undergo a background check provided by a third-party screening company, upon hire.	No exceptions noted.
		Performance management procedures are documented to give guidance to personnel on the overall continuous performance management process.	Inspected the performance management procedures to determine that performance management procedures were documented to give guidance to personnel on the overall continuous performance management process.	No exceptions noted.
		The entity employs the progressive discipline approach, which includes individual coaching and a PIP, for any personnel failing to meet entity standards for work performance.	Inspected the performance management procedures to determine that the entity employed the progressive discipline approach, which included individual coaching and a PIP, for any personnel failing to meet entity standards for work performance.	No exceptions noted.
		The entity utilizes a continuous performance management approach for personnel to assess their performance and provide feedback via various meetings throughout the year, but no less than annually.	Inquired of the Security Analyst regarding performance management to determine that the entity utilized a continuous performance management approach for personnel to assess their performance and provided feedback via various meetings throughout the year, but no less than annually.	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 performance management procedures to determine that the entity utilized a continuous performance management approach for personnel to assess their performance and provided feedback via various meetings throughout the year, but no less than annually.	No exceptions noted.
			Inspected the completed performance management documentation for a sample of current employees to determine that the entity utilized a continuous performance management approach for personnel to assess their performance and provided feedback via various meetings throughout the year, but no less than annually.	No exceptions noted.
		The entity provides various training programs, including continuing education and security awareness training, through a LMS to ensure skill sets and technical competency of personnel are developed and maintained.	Inspected the LMS dashboard and the course completion log for the population of personnel for the entire review period to determine that the entity provided various training programs, including continuing education and security awareness training, through a LMS to ensure skill sets and technical competency of personnel were developed and maintained.	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 are required to complete security awareness training upon hire and annually thereafter.	Inquired of the Security Analyst regarding the hiring process to determine that personnel were required to complete security awareness training upon hire and annually thereafter.	No exceptions noted.
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that personnel were required to complete security awareness training upon hire and annually thereafter.	No exceptions noted.
			Inspected the course completion log for a sample of new hires to determine that personnel were required to complete security awareness training upon hire and annually thereafter.	No exceptions noted.
			Inspected the course completion log for a sample of current employees to determine that personnel were required to complete security awareness training upon hire and annually thereafter.	No exceptions noted.
		Changes or updates to the overall training programs delivered to personnel are assessed at least annually by management.	Inspected the content review meeting invite and agenda to determine that changes or updates to the overall training programs delivered to personnel were assessed at least annually by 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**
		The entity evaluates the competencies and experience of third-party vendors prior to working with them.	Inquired of the Security Analyst regarding the third-party vendor risk assessment process to determine that the entity evaluated the competencies and experience of third-party vendors prior to working with them.	No exceptions noted.
			Inspected the vendor risk management policy to determine that the entity evaluated the competencies and experience of third-party vendors prior to working with them.	No exceptions noted.
			Inspected the vendor risk analysis for a sample of new third-party vendors to determine that the entity evaluated the competencies and experience of third-party vendors prior to working with them.	Testing of the control activity disclosed that no new third-party vendors were onboarded during the review period.

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.	The entity maintains an organizational chart and job descriptions for personnel, including executive management, to delineate reporting lines and other related responsibilities. The organizational chart and job descriptions are reviewed periodically throughout the year, but no less than annually, and made available to personnel to enable awareness of their responsibilities.	Inspected the organizational chart, including revision history, job description for the population of job roles, including date of last review, and the entity's intranet site to determine that the entity maintained an organizational chart and job descriptions for personnel, including executive management, to delineate reporting lines and other related responsibilities, and that the organizational chart and job descriptions were reviewed periodically throughout the year, but no less than annually, and made available to personnel to enable awareness of their responsibilities.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook upon hire and annually thereafter.	Inquired of the Security Analyst regarding the hiring process to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	No exceptions noted.
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	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 completed employee handbook acknowledgement log for a sample of new hires to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	No exceptions noted.
			Inspected the completed employee handbook acknowledgement log for a sample of current employees to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	No exceptions noted.
		Performance management procedures are documented to give guidance to personnel on the overall continuous performance management process.	Inspected the performance management procedures to determine that performance management procedures were documented to give guidance to personnel on the overall continuous performance management process.	No exceptions noted.
		The entity employs the progressive discipline approach, which includes individual coaching and a PIP, for any personnel failing to meet entity standards for work performance.	Inspected the performance management procedures to determine that the entity employed the progressive discipline approach, which included individual coaching and a PIP, for any personnel failing to meet entity standards for work performance.	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 entity utilizes a continuous performance management approach for personnel to assess their performance and provide feedback via various meetings throughout the year, but no less than annually.	Inquired of the Security Analyst regarding performance management to determine that the entity utilized a continuous performance management approach for personnel to assess their performance and provided feedback via various meetings throughout the year, but no less than annually.	No exceptions noted.
			Inspected the performance management procedures to determine that the entity utilized a continuous performance management approach for personnel to assess their performance and provided feedback via various meetings throughout the year, but no less than annually.	No exceptions noted.
			Inspected the completed performance management documentation for a sample of current employees to determine that the entity utilized a continuous performance management approach for personnel to assess their performance and provided feedback via various meetings throughout the year, but no less than annually.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Control Environment</th></tr>
<tr><th>CC1.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>The employee handbook communicates workforce conduct standards and enforcement procedures, which include disciplinary actions, up to and including termination as potential sanctions for employee misconduct or violations.</td><td>Inspected the employee handbook to determine that the employee handbook communicated workforce conduct standards and enforcement procedures, which included disciplinary actions, up to and including termination as potential sanctions for employee misconduct or violations.</td><td>No exceptions noted.</td></tr>
</table>

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 entity has documented policies and procedures in support of the internal controls and objectives, which communicate control responsibilities and define system boundaries to personnel and are made available through the entity's intranet site.	Inspected the entity's policies and procedures and the entity's intranet site to determine that the entity had documented policies and procedures in support of the internal controls and objectives, which communicated control responsibilities and defined system boundaries to personnel and were made available through the entity's intranet site.	No exceptions noted.
		Data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the data flow diagrams to determine that data flow diagrams were documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
		Data entered into the system, processed by the system, and output from the system is protected from unauthorized access.	Inspected the load balancer listeners, certificates, TLS settings, IDS configurations, the encryption configurations for data at rest, and the FIM rules to determine that data entered into the system, processed by the system, and output from the system was protected from unauthorized access.	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**
		Policies and procedures are in place that give guidance to personnel on the retention, handling, classification, and disposal of information and devices.	Inspected the data retention, destruction, backup and relevance policy and the data classification policy to determine that policies and procedures were in place that gave guidance to personnel on the retention, handling, classification, and disposal of information and devices.	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 entity has documented policies and procedures in support of the internal controls and objectives, which communicate control responsibilities and define system boundaries to personnel and are made available through the entity's intranet site.	Inspected the entity's policies and procedures and the entity's intranet site to determine that the entity had documented policies and procedures in support of the internal controls and objectives, which communicated control responsibilities and defined system boundaries to personnel and were made available through the entity's intranet site.	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 entity maintains an organizational chart and job descriptions for personnel, including executive management, to delineate reporting lines and other related responsibilities. The organizational chart and job descriptions are reviewed periodically throughout the year, but no less than annually, and made available to personnel to enable awareness of their responsibilities.	Inspected the organizational chart, including revision history, job description for the population of job roles, including date of last review, and the entity's intranet site to determine that the entity maintained an organizational chart and job descriptions for personnel, including executive management, to delineate reporting lines and other related responsibilities, and that the organizational chart and job descriptions were reviewed periodically throughout the year, but no less than annually, and made available to personnel to enable awareness of their responsibilities.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook upon hire and annually thereafter.	Inquired of the Security Analyst regarding the hiring process to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	No exceptions noted.
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that personnel were required to acknowledge the employee handbook upon hire 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
			Inspected the completed employee handbook acknowledgement log for a sample of new hires to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	No exceptions noted.
			Inspected the completed employee handbook acknowledgement log for a sample of current employees to determine that personnel were required to acknowledge the employee handbook upon hire and annually thereafter.	No exceptions noted.
		The entity provides various training programs, including continuing education and security awareness training, through a LMS to ensure skill sets and technical competency of personnel are developed and maintained.	Inspected the LMS dashboard and the course completion log for the population of personnel for the entire review period to determine that the entity provided various training programs, including continuing education and security awareness training, through a LMS to ensure skill sets and technical competency of personnel were developed and maintained.	No exceptions noted.
		Personnel are required to complete security awareness training upon hire and annually thereafter.	Inquired of the Security Analyst regarding the hiring process to determine that personnel were required to complete security awareness training upon hire 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**
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that personnel were required to complete security awareness training upon hire and annually thereafter.	No exceptions noted.
			Inspected the course completion log for a sample of new hires to determine that personnel were required to complete security awareness training upon hire and annually thereafter.	No exceptions noted.
			Inspected the course completion log for a sample of current employees to determine that personnel were required to complete security awareness training upon hire and annually thereafter.	No exceptions noted.
		The Board of Directors meet with senior management quarterly to provide overall governance support to the entity.	Inspected the Board of Directors meeting minutes for a sample of quarters to determine that the Board of Directors met with senior management quarterly to provide overall governance support to the entity.	No exceptions noted.
		An anonymous hotline is in place to allow employees, third parties, and customers to report unethical behavior in a confidential and anonymous manner.	Inquired of the Security Analyst regarding unethical behavior to determine that an anonymous hotline was in place to allow employees, third parties, and customers to report unethical behavior in a confidential and anonymous manner.	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 employee handbook and the terms and conditions page on the entity's externally-facing website to determine that an anonymous hotline was in place to allow employees, third parties, and customers to report unethical behavior in a confidential and anonymous manner.	No exceptions noted.
		Policies and procedures are in place that include defined responsibilities, communication protocols, and give guidance to personnel over the investigation, evaluation, documentation, and resolution of an incident. The policies and procedures are made available to personnel and reviewed at least annually.	Inspected the information protection policy, the incident response policy, the issue tracking policy, and the entity's intranet site to determine that policies and procedures were in place that included defined responsibilities, communication protocols, and gave guidance to personnel over the investigation, evaluation, documentation, and resolution of an incident, and that the policies and procedures were made available to personnel and reviewed at least annually.	No exceptions noted.
		Entity performance, updates, and objectives, including changes made to the objectives, are communicated to personnel through the entity's quarterly full team update meeting.	Inspected the full team update meeting slide deck and associated meeting invite for a sample of quarters to determine that entity performance, updates, and objectives, including changes made to the objectives, were communicated to personnel through the entity's quarterly full team update meeting.	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**
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Third-party agreements outline and communicate the system commitments, requirements, terms, conditions and responsibilities of third-party vendors.	Inspected the agreement for a sample of third-party vendors to determine that third-party agreements outlined and communicated the system commitments, requirements, terms, conditions and responsibilities of third-party vendors.	No exceptions noted.
		Commitments and requirements related to security, confidentiality, responsibilities, and terms of the relationship for contractors with system access, are outlined in the contractor agreement.	Inquired of the Security Analyst regarding contractors to determine that commitments and requirements related to security, confidentiality, responsibilities, and terms of the relationship for contractors with system access, were outlined in the contractor agreement.	No exceptions noted.
			Inspected the contractor agreement for the population of contractors with system access to determine that commitments and requirements related to security, confidentiality, responsibilities, and terms of the relationship for contractors with system access, were outlined in the contractor agreement.	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
		Customer commitments, requirements, and responsibilities are outlined and communicated through the entity's online terms and conditions and the master content subscription agreements (MCSA), if applicable.	Inspected the terms and conditions on the entity's externally-facing website and the sales order and MCSA, if applicable, for a sample of customers to determine that customer commitments, requirements, and responsibilities were outlined and communicated through the entity's online terms and conditions and the MCSA, if applicable.	No exceptions noted.
		Contact information for the entity's Support team is available via the externally-facing website and within the application, which enables external parties to ask questions, report issues, and review various resources.	Inquired of the Vice President and Chief Technology Officer regarding external parties to determine that contact information for the entity's Support team was available via the externally-facing website and within the application, which enabled external parties to ask questions, report issues, and review various resources.	No exceptions noted.
			Inspected the support channels within the application and the support page on the externally-facing website to determine that contact information for the entity's Support team was available via the externally-facing website and within the application, which enabled external parties to ask questions, report issues, and review various resources.	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 anonymous hotline is in place to allow employees, third parties, and customers to report unethical behavior in a confidential and anonymous manner.	Inquired of the Security Analyst regarding unethical behavior to determine that an anonymous hotline was in place to allow employees, third parties, and customers to report unethical behavior in a confidential and anonymous manner.	No exceptions noted.
			Inspected the employee handbook and the terms and conditions page on the entity's externally-facing website to determine that an anonymous hotline was in place to allow employees, third parties, and customers to report unethical behavior in a confidential and anonymous manner.	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 entity establishes objectives that are reflective of management's choices about growth, innovation, entity structure, the industry, and performance of the entity.	Inspected the entity's objectives to determine that the entity established objectives that were reflective of management's choices about growth, innovation, entity structure, the industry, and performance of the entity.	No exceptions noted.
		The established objectives by management are specific, measurable, attainable, relevant, and time-bound.	Inspected the entity's objectives to determine that the entity established objectives that the established objectives by management were specific, measurable, attainable, relevant, and time-bound.	No exceptions noted.
		Various metrics indicative of entity performance is documented and tracked by management.	Inquired of the Vice President and Chief Technology Officer regarding entity performance to determine that various metrics indicative of entity performance were documented and tracked by management.	No exceptions noted.
			Inspected the full team update meeting slide deck and associated meeting invite for a sample of quarters to determine that various metrics indicative of entity performance were documented and tracked by management.	No exceptions noted.
			Inspected the weekly Leadership team recurring meeting invite, running meeting agenda, and meeting minutes for the entire review period to determine that various metrics indicative of entity performance were documented and tracked by 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**
		The Leadership team meets weekly to review and discuss financial metrics, entity performance, resources, and business plans to ensure alignment with the corporate goals and objectives.	Inspected the weekly Leadership team recurring meeting invite, running meeting agenda, and meeting minutes for the entire review period to determine that the Leadership Team met weekly to review and discuss financial metrics, entity performance, resources, and business plans to ensure alignment with the corporate goals and objectives.	No exceptions noted.
		The entity utilizes a GRC tool to manage internal risk and compliance activities and risks associated with external parties. At least annually, personnel with risk management responsibilities assess changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives in the GRC tool.	Inquired of the Vice President and Chief Technology Officer regarding risk management procedures to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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
			Observed the workflows and risk management processes of the GRC tool to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	No exceptions noted.
			Inspected the completed risk assessment report to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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 IT team is responsible for coordinating and ensuring the risk assessment process is done in accordance with the risk management policy.	Inspected the risk management policy to determine that the IT team was responsible for coordinating and ensuring the risk assessment process was done in accordance with the risk management policy.	No exceptions noted.
		The entity's internal controls environment is based on the Security Controls Framework (SCF) and takes into consideration various statutory, regulatory, and contractual requirements.	Inspected the data privacy legal and contractual requirements policy and the completed internal controls matrix to determine that the entity's internal controls environment was based on the SCF and took into consideration various statutory, regulatory, and contractual requirements.	No exceptions noted.
		A third-party performs an independent assessment of the entity's controls environment annually to assess the effectiveness of internal controls implemented within the environment and to show compliance to relevant laws, regulations and standards.	Inspected the entity's completed attestation report to determine that a third-party performed an independent assessment of the entity's controls environment annually to assess the effectiveness of internal controls implemented within the environment and to show compliance to relevant laws, regulations and standards.	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**
CC3.2	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 risk management policy and issue tracking policy contain procedures around the risk management process to guide personnel in identifying threats and vulnerabilities, evaluating and addressing risks, defining specified risk tolerances, and risk mitigation.	Inspected the risk management policy and issue tracking policy to determine that the risk management policy and issue tracking policy contained procedures around the risk management process to guide personnel in identifying threats and vulnerabilities, evaluating and addressing risks, defining specified risk tolerances, and risk mitigation.	No exceptions noted.
		The IT team is responsible for coordinating and ensuring the risk assessment process is done in accordance with the risk management policy.	Inspected the risk management policy to determine that the IT team was responsible for coordinating and ensuring the risk assessment process was done in accordance with the risk management policy.	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 entity utilizes a GRC tool to manage internal risk and compliance activities and risks associated with external parties. At least annually, personnel with risk management responsibilities assess changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives in the GRC tool.	Inquired of the Vice President and Chief Technology Officer regarding risk management procedures to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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**
			Observed the workflows and risk management processes of the GRC tool to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	No exceptions noted.
			Inspected the completed risk assessment report to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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
		Risks identified as part of the risk management process are evaluated by determining the initial impact and likelihood of the risk as if no controls are in place to establish the maximum risk, determining the controls and mitigating factors in place, then reevaluating the risk impact and likelihood with controls and mitigating factors present to establish the overall residual risk level.	Inquired of the Vice President and Chief Technology Officer regarding risk management procedures to determine that risks identified as part of the risk management process were evaluated by determining the initial impact and likelihood of the risk as if no controls were in place to establish the maximum risk, determining the controls and mitigating factors in place, then reevaluating the risk impact and likelihood with controls and mitigating factors present to establish the overall residual risk level.	No exceptions noted.
			Observed the workflows and risk management processes of the GRC tool to determine that risks identified as part of the risk management process were evaluated by determining the initial impact and likelihood of the risk as if no controls were in place to establish the maximum risk, determining the controls and mitigating factors in place, then reevaluating the risk impact and likelihood with controls and mitigating factors present to establish the overall residual risk level.	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**
			Inspected the completed risk assessment report to determine that risks identified as part of the risk management process were evaluated by determining the initial impact and likelihood of the risk as if no controls were in place to establish the maximum risk, determining the controls and mitigating factors in place, then reevaluating the risk impact and likelihood with controls and mitigating factors present to establish the overall residual risk level.	No exceptions noted.
		Issues identified from the various evaluations performed are tracked by management through the GRC tool or ticketing system to ensure they are addressed in a timely manner.	Inquired of the Vice President and Chief Technology Officer regarding issue management to determine that issues identified from the various evaluations performed were tracked by management through the GRC tool or ticketing system to ensure they were addressed in a timely manner.	No exceptions noted.
			Inspected the issue tracking policy to determine that issues identified from the various evaluations performed were tracked by management through the GRC tool or ticketing system to ensure they were addressed in a timely manner.	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**
			Inspected the issues board within the GRC tool and ticketing system to determine that issues identified from the various evaluations performed were tracked by management through the GRC tool or ticketing system to ensure they were addressed in a timely manner.	No exceptions noted.
		The Security team meets on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	Inquired of the Vice President and Chief Technology Officer regarding the Security team to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the issue tracking policy to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the Security team meeting minutes for a sample of months to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	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 performs annual due diligence procedures on third-party vendors who are classified as a sub-processor. Monitoring procedures include maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	Inquired of the Security Analyst regarding the third-party vendor risk assessment process to determine that management performed annual due diligence procedures on third-party vendors who were classified as a sub-processor, and that monitoring procedures included maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	No exceptions noted.
			Inspected the vendor risk management policy to determine that management performed annual due diligence procedures on third-party vendors who were classified as a sub-processor, and that monitoring procedures included maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	No exceptions noted.
			Inspected the listing of third-party sub-processors, attestation report, and vendor attestation report review meeting minutes for a sample of third-party vendors to determine that management performed annual due diligence procedures on third-party vendors who were classified as a sub-processor, and that monitoring procedures included maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	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**
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The entity utilizes a GRC tool to manage internal risk and compliance activities and risks associated with external parties. At least annually, personnel with risk management responsibilities assess changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives in the GRC tool.	Inquired of the Vice President and Chief Technology Officer regarding risk management procedures to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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**
			Observed the workflows and risk management processes of the GRC tool to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	No exceptions noted.
			Inspected the completed risk assessment report to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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 assessment of fraud related risks includes the consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information.	Inquired of the Vice President and Chief Technology Officer regarding risk management procedures to determine that the assessment of fraud related risks included the consideration of threats and vulnerabilities that arose specifically from the use of IT and access to information.	No exceptions noted.
			Observed the workflows and risk management processes of the GRC tool to determine that the assessment of fraud related risks included the consideration of threats and vulnerabilities that arose specifically from the use of IT and access to information.	No exceptions noted.
			Inspected the completed risk assessment report to determine that the assessment of fraud related risks included the consideration of threats and vulnerabilities that arose specifically from the use of IT and access to information.	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 entity utilizes a GRC tool to manage internal risk and compliance activities and risks associated with external parties. At least annually, personnel with risk management responsibilities assess changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives in the GRC tool.	Inquired of the Vice President and Chief Technology Officer regarding risk management procedures to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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**
			Observed the workflows and risk management processes of the GRC tool to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	No exceptions noted.
			Inspected the completed risk assessment report to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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 in the external environment are considered and evaluated as part of the risk management activities.	Inquired of the Vice President and Chief Technology Officer regarding risk management procedures to determine that changes in the external environment were considered and evaluated as part of the risk management activities.	No exceptions noted.
			Observed the workflows and risk management processes of the GRC tool to determine that changes in the external environment were considered and evaluated as part of the risk management activities.	No exceptions noted.
			Inspected the completed risk assessment report to determine that changes in the external environment were considered and evaluated as part of the risk management 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**
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.	System logging and monitoring software is used to collect data from system infrastructure components and endpoints, and to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity. Alerts are sent to personnel when certain alarms are triggered.	Inspected the monitoring software configurations, rules, simple notification service (SNS) topics, alert settings, integrations, and example alerts to determine that system logging and monitoring software was used to collect data from system infrastructure components and endpoints, and to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity, and that alerts were sent to personnel when certain alarms were triggered.	No exceptions noted.
		Entity policies and procedures are reviewed at least annually for accuracy and applicability to the current functioning of internal controls.	Inquired of the Security Analyst regarding entity policies and procedures to determine that entity policies and procedures were reviewed at least annually for accuracy and applicability to the current functioning of internal controls.	No exceptions noted.
			Inspected the entity's policies and procedures including revision history to determine that the entity had documented policies and procedures in support of the internal controls and objectives, which communicated control responsibilities and defined system boundaries to personnel and were made available through the entity's intranet site.	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 Security team meets on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	Inquired of the Vice President and Chief Technology Officer regarding the Security team to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the issue tracking policy to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the Security team meeting minutes for a sample of months to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
		Logical access privileges are reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts.	Inquired of the Senior Manager of Information Technology regarding access reviews to determine that logical access privileges were reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts.	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**
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that logical access privileges were reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts.	No exceptions noted.
			Inspected the completed user account review documentation for the in-scope systems for a sample of quarters to determine that logical access privileges were reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts.	No exceptions noted.
		A backup restoration test is performed on an annual basis.	Inquired of the Security Analyst regarding restore testing to determine that a backup restoration test was performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test results and restore test script to determine that a backup restoration test was performed on an annual basis.	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**
		A third-party vulnerability scanning tool is utilized to continuously scan assets for vulnerabilities.	Inquired of the Security Analyst regarding vulnerability scanning to determine that a third-party vulnerability scanning tool was utilized to continuously scan assets for vulnerabilities.	No exceptions noted.
			Inspected the vulnerability scanning tool schedule, scan activity report, and an example executive summary report to determine that a third-party vulnerability scanning tool was utilized to continuously scan assets for vulnerabilities.	No exceptions noted.
		A third-party performs a penetration test annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test report to determine that a third-party performed a penetration test annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		The entity utilizes a continuous performance management approach for personnel to assess their performance and provide feedback via various meetings throughout the year, but no less than annually.	Inquired of the Security Analyst regarding performance management to determine that the entity utilized a continuous performance management approach for personnel to assess their performance and provided feedback via various meetings throughout the year, but no less than annually.	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**
			Inspected the performance management procedures to determine that the entity utilized a continuous performance management approach for personnel to assess their performance and provided feedback via various meetings throughout the year, but no less than annually.	No exceptions noted.
			Inspected the completed performance management documentation for a sample of current employees to determine that the entity utilized a continuous performance management approach for personnel to assess their performance and provided feedback via various meetings throughout the year, but no less than annually.	No exceptions noted.
		Management performs annual due diligence procedures on third-party vendors who are classified as a sub-processor. Monitoring procedures include maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	Inquired of the Security Analyst regarding the third-party vendor risk assessment process to determine that management performed annual due diligence procedures on third-party vendors who were classified as a sub-processor, and that monitoring procedures included maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	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
			Inspected the vendor risk management policy to determine that management performed annual due diligence procedures on third-party vendors who were classified as a sub-processor, and that monitoring procedures included maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	No exceptions noted.
			Inspected the listing of third-party sub-processors, attestation report, and vendor attestation report review meeting minutes for a sample of third-party vendors to determine that management performed annual due diligence procedures on third-party vendors who were classified as a sub-processor, and that monitoring procedures included maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	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 entity utilizes a GRC tool to manage internal risk and compliance activities and risks associated with external parties. At least annually, personnel with risk management responsibilities assess changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives in the GRC tool.	Inquired of the Vice President and Chief Technology Officer regarding risk management procedures to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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
			Observed the workflows and risk management processes of the GRC tool to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	No exceptions noted.
			Inspected the completed risk assessment report to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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 IT team is responsible for coordinating and ensuring the risk assessment process is done in accordance with the risk management policy.	Inspected the risk management policy to determine that the IT team was responsible for coordinating and ensuring the risk assessment process was done in accordance with the risk management policy.	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 Security team meets on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	Inquired of the Vice President and Chief Technology Officer regarding the Security team to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the issue tracking policy to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the Security team meeting minutes for a sample of months to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	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**
		Deficiencies identified from the various assessments performed on the environment are documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	Inquired of the Vice President and Chief Technology Officer regarding deficiencies to determine that deficiencies identified from the various assessments performed on the environment were documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	No exceptions noted.
			Inspected the issue tracking policy to determine that deficiencies identified from the various assessments performed on the environment were documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	No exceptions noted.
			Inspected the completed risk assessment report, completed penetration test report, vulnerability scanning tool schedule, scan activity report, and an example executive summary report to determine that deficiencies identified from the various assessments performed on the environment were documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	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**
			Inspected the deviation remediation documentation for a sample of deviations identified from monitoring tools to determine that deficiencies identified from the various assessments performed on the environment were documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	No exceptions noted.
			Inspected the vulnerability remediation documentation for the population of vulnerabilities identified from the vulnerability scanning tool and penetration test to determine that deficiencies identified from the various assessments performed on the environment were documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	No exceptions noted.
			Inspected the control failure remediation documentation for a sample of control failures to determine that deficiencies identified from the various assessments performed on the environment were documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	Testing of the control activity disclosed that no control failures occurred during the review period.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Monitoring Activities</th></tr>
<tr><th>CC4.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>Issues identified from the various evaluations performed are tracked by management through the GRC tool or ticketing system to ensure they are addressed in a timely manner.</td><td>Inquired of the Vice President and Chief Technology Officer regarding issue management to determine that issues identified from the various evaluations performed were tracked by management through the GRC tool or ticketing system to ensure they were addressed in a timely manner.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the issue tracking policy to determine that issues identified from the various evaluations performed were tracked by management through the GRC tool or ticketing system to ensure they were addressed in a timely manner.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the issues board within the GRC tool and ticketing system to determine that issues identified from the various evaluations performed were tracked by management through the GRC tool or ticketing system to ensure they were addressed in a timely manner.</td><td>No exceptions noted.</td></tr>
</table>

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.	Management has documented the controls in place for each relevant business process of the various levels in the entity and incorporated a variety of controls into the environment that include, but are not limited to, manual and automated controls, which are assigned to process owners based on job role.	Inspected the completed internal controls matrix to determine that management had documented the controls in place for each relevant business process of the various levels in the entity and incorporated a variety of controls into the environment that included, but were not limited to, manual and automated controls, which were assigned to process owners based on job role.	No exceptions noted.
		The Security team meets on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	Inquired of the Vice President and Chief Technology Officer regarding the Security team to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the issue tracking policy to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Control Activities</th></tr>
<tr><th>CC5.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td></td><td>Inspected the Security team meeting minutes for a sample of months to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>The entity utilizes a GRC tool to manage internal risk and compliance activities and risks associated with external parties. At least annually, personnel with risk management responsibilities assess changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives in the GRC tool.</td><td>Inquired of the Vice President and Chief Technology Officer regarding risk management procedures to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.</td><td>No exceptions noted.</td></tr>
</table>

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
			Observed the workflows and risk management processes of the GRC tool to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	No exceptions noted.
			Inspected the completed risk assessment report to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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
		Deficiencies identified from the various assessments performed on the environment are documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	Inquired of the Vice President and Chief Technology Officer regarding deficiencies to determine that deficiencies identified from the various assessments performed on the environment were documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	No exceptions noted.
			Inspected the issue tracking policy to determine that deficiencies identified from the various assessments performed on the environment were documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	No exceptions noted.
			Inspected the completed risk assessment report, completed penetration test report, vulnerability scanning tool schedule, scan activity report, and an example executive summary report to determine that deficiencies identified from the various assessments performed on the environment were documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	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**
			Inspected the deviation remediation documentation for a sample of deviations identified from monitoring tools to determine that deficiencies identified from the various assessments performed on the environment were documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	No exceptions noted.
			Inspected the vulnerability remediation documentation for the population of vulnerabilities identified from the vulnerability scanning tool and penetration test to determine that deficiencies identified from the various assessments performed on the environment were documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	No exceptions noted.
			Inspected the control failure remediation documentation for a sample of control failures to determine that deficiencies identified from the various assessments performed on the environment were documented, communicated to those parties responsible for taking corrective actions, investigated, and addressed.	Testing of the control activity disclosed that no control failures occurred during the review period.

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 entity has documented policies and procedures in support of the internal controls and objectives, which communicate control responsibilities and define system boundaries to personnel and are made available through the entity's intranet site.	Inspected the entity's policies and procedures and the entity's intranet site to determine that the entity had documented policies and procedures in support of the internal controls and objectives, which communicated control responsibilities and defined system boundaries to personnel and were made available through the entity's intranet site.	No exceptions noted.
		Management has documented control activities over the entity's technology infrastructure to support the achievement of objectives.	Inspected the completed internal controls matrix to determine that management had documented control activities over the entity's technology infrastructure to support the achievement of objectives.	No exceptions noted.
		Management has documented control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.	Inspected the completed internal controls matrix to determine that management had documented control activities that were designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.	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**
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The entity has documented policies and procedures in support of the internal controls and objectives, which communicate control responsibilities and define system boundaries to personnel and are made available through the entity's intranet site.	Inspected the entity's policies and procedures and the entity's intranet site to determine that the entity had documented policies and procedures in support of the internal controls and objectives, which communicated control responsibilities and defined system boundaries to personnel and were made available through the entity's intranet site.	No exceptions noted.
		The entity maintains an organizational chart and job descriptions for personnel, including executive management, to delineate reporting lines and other related responsibilities. The organizational chart and job descriptions are reviewed periodically throughout the year, but no less than annually, and made available to personnel to enable awareness of their responsibilities.	Inspected the organizational chart, including revision history, job description for the population of job roles, including date of last review, and the entity's intranet site to determine that the entity maintained an organizational chart and job descriptions for personnel, including executive management, to delineate reporting lines and other related responsibilities, and that the organizational chart and job descriptions were reviewed periodically throughout the year, but no less than annually, and made available to personnel to enable awareness of their responsibilities.	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 Security team meets on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	Inquired of the Vice President and Chief Technology Officer regarding the Security team to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the issue tracking policy to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the Security team meeting minutes for a sample of months to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	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.	Policies and procedures are in place that give guidance to personnel on system settings, authentication, access, and security monitoring.	Inspected the information protection policy, the issue tracking policy, and the onboarding, offboarding, user access, and user access review policy to determine that policies and procedures were in place that gave guidance to personnel on system settings, authentication, access, and security monitoring.	No exceptions noted.
		The entity identifies, inventories, classifies, and manages information assets.	Inspected the hardware and software inventory listing to determine that the entity identified, inventoried, classified, and managed information assets.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Senior Manager of Information Technology regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	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 user listings for the in-scope systems and the access request documentation for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the user listings for the in-scope systems and the access request documentation for the population of new contractors granted access to the in-scope systems to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Senior Manager of Information Technology regarding the termination process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that logical access to systems was revoked as a component of the termination process.	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 user listings for the in-scope systems and the access revocation documentation for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the user listings for the in-scope systems and the access revocation documentation for the population of terminated contractors with access to the in-scope systems to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
	Google Workspace			
		Google Workspace user access is restricted via role-based security privileges defined within the access control system.	Inspected the Google Workspace user listing, including associated role, to determine that Google Workspace user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Google Workspace administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Senior Manager of Information Technology regarding administrative access to Google Workspace to determine that Google Workspace administrative access was restricted to user accounts accessible by 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**
			Inspected the Google Workspace administrator listing to determine that Google Workspace administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Users are authenticated through Okta prior to being able to access the network and any Okta integrated applications through SSO. Users are required to separately sign on to any systems or applications that do not use the SSO functionality of Okta. Okta is configured to enforce the following security requirements: • Password history • Minimum password length • Complexity requirements • Common password check • Account lockout threshold • MFA	Inquired of the Senior Manager of Information Technology regarding network access to determine that users were authenticated through Okta prior to being able to access the network and any Okta integrated applications through SSO; users were required to separately sign on to any systems or applications that did not use the SSO functionality of Okta, and that Okta was configured to enforce the following security requirements: • Password history • Minimum password length • Complexity requirements • Common password check • Account lockout threshold • MFA	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Logical and Physical Access Controls</th></tr>
<tr><th>CC6.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td></td><td>Observed the authentication of a user through Okta to determine that users were authenticated through Okta prior to being able to access the network and any Okta integrated applications through SSO; users were required to separately sign on to any systems or applications that did not use the SSO functionality of Okta, and that Okta was configured to enforce the following security requirements:
• Password history
• Minimum password length
• Complexity requirements
• Common password check
• Account lockout threshold
• MFA</td><td>No exceptions noted.</td></tr>
</table>

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 Okta directory integrations, Okta MFA policy, and Okta password policy to determine that users were authenticated through Okta prior to being able to access the network and any Okta integrated applications through SSO; users were required to separately sign on to any systems or applications that did not use the SSO functionality of Okta, and that Okta was configured to enforce the following security requirements: • Password history • Minimum password length • Complexity requirements • Common password check • Account lockout threshold • MFA	No exceptions noted.
	GCP			
		GCP access and associated user permissions are managed via IAM. Access to GCP is restricted to the administrators.	Inquired of the Senior Manager of Information Technology regarding access to GCP to determine that GCP access and associated user permissions were managed via IAM, and that access to GCP was restricted to the administrators.	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 GCP member listing, including associated roles, to determine that GCP access and associated user permissions were managed via IAM, and that access to GCP was restricted to the administrators.	No exceptions noted.
		GCP is configured to enforce the following security settings: • Minimum password length • Maximum password length • Enforce strong password • Two-Factor Authentication (2FA)	Inspected the GCP security settings to determine that Google Workspace and GCP were configured to enforce the following security settings: • Minimum password length • Maximum password length • Enforce strong password • 2FA	No exceptions noted.
	AWS			
		AWS user access and associated user permissions are managed via IAM.	Inspected the AWS user listing, including associated groups, to determine that AWS user access and associated user permissions were managed via IAM.	No exceptions noted.
		AWS administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Vice President and Chief Technology Officer regarding administrative access to AWS to determine that AWS administrative access was restricted to user accounts accessible by 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**
			Inspected the AWS administrator listing, including associated policies, to determine that AWS administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		AWS management console access is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password length • At least one uppercase letter • At least one lowercase letter • At least one number • At least one non-alphanumeric character	Inspected the AWS password policy to determine that AWS management console access was configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password length • At least one uppercase letter • At least one lowercase letter • At least one number • At least one non-alphanumeric character	No exceptions noted.
		AWS users are required to authenticate via MFA.	Inquired of the Vice President and Chief Technology Officer regarding authentication to AWS to determine that AWS users were required to authenticate via MFA.	No exceptions noted.
			Inspected the MFA policy and AWS user listing to determine that AWS users were required to authenticate via MFA.	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 keys are used to authenticate to the AWS command line interface (CLI).	Inquired of the Vice President and Chief Technology Officer regarding authentication to AWS to determine that access keys were used to authenticate to the AWS CLI.	No exceptions noted.
			Inspected the AWS CLI settings and access keys to determine that access keys were used to authenticate to the AWS CLI.	No exceptions noted.
		AWS audit logging is configured to log various actions across the AWS infrastructure, including any application programing interface (API) and management console activity.	Inspected the AWS trails and an example AWS event history log to determine that AWS audit logging was configured to log various actions across the AWS infrastructure, including any API and management console activity.	No exceptions noted.
	Operating System (Linux and Windows)			
		Operating system users are managed through the defined IAM policies.	Inquired of the Vice President and Chief Technology Officer regarding the operating system to determine that operating system users were managed via the defined IAM policies.	No exceptions noted.
			Inspected the operating system user listing, including associated groups, to determine that operating system users were managed via the defined IAM policies.	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 to the operating system was via AWS Systems Manager Session Manager.	Inquired of the Vice President and Chief Technology Officer regarding the operating system to determine that access to the operating system was via AWS Systems Manager Session Manager.	No exceptions noted.
			Observed the authentication of a user to the operating system to determine that access to the operating system was via AWS Systems Manager Session Manager.	No exceptions noted.
			Inspected the AWS Systems Manager dashboard and an example session history log to determine that access to the operating system was via AWS Systems Manager Session Manager.	No exceptions noted.
		Operating system audit logging is in place that tracks user activity.	Inquired of the Vice President and Chief Technology Officer regarding the operating system to determine that operating system audit logging was in place that tracked user activity.	No exceptions noted.
			Inspected the operating system audit logging configurations and an example operating system audit log to determine that operating system audit logging was in place that tracked user activity.	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
	Database (AWS RDS MySQL)			
		Database users are managed and authenticated through the defined IAM policies.	Inquired of the Vice President and Chief Technology Officer regarding the database to determine that database users were managed and authenticated through the defined IAM policies.	No exceptions noted.
			Observed the authentication of a user to the database to determine that database users were managed and authenticated through the defined IAM policies.	No exceptions noted.
			Inspected the AWS user listing, including associated groups and user classes, and the roles and permissions for the database to determine that database users were managed and authenticated through the defined IAM policies.	No exceptions noted.
		The database is configured to log server activity, which includes when clients connect, disconnect, and activity performed while connected.	Inspected the database audit logging configurations and an example database audit log to determine that the database was configured to log server activity, which included when clients connected, disconnected, and activity performed while connected.	No exceptions noted.
	Application (OpenSesame)			
		Application user access is restricted via role-based security privileges.	Inspected the application user listing, including associated roles, to determine that application user access was restricted via role-based security privileges.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Logical and Physical Access Controls</th></tr>
<tr><th>CC6.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>Application administrative access is restricted to user accounts accessible by authorized personnel.</td><td>Inquired of the Vice President and Chief Technology Officer regarding administrative access to the application to determine that application administrative access was restricted to user accounts accessible by authorized personnel.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the application administrator listing, including associated roles, to determine that application administrative access was restricted to user accounts accessible by authorized personnel.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Users are authenticated to the application based on the requirements set for the identity provider. The identity provider is configured to enforce the following requirements:
• Password history
• Minimum password length
• Complexity requirements
• Common password check
• Account lockout threshold</td><td>Inspected the application configurations and identity provider security settings to determine that users were authenticated to the application based on the requirements set for the identity provider, and that the identity provider was configured to enforce the following requirements:
• Password history
• Minimum password length
• Complexity requirements
• Common password check
• Account lockout threshold</td><td>No exceptions noted.</td></tr>
</table>

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
		Logging is configured for the application to log any user activity and system events.	Inspected the application audit logging configurations and an example application log to determine that logging was configured for the application to log any user activity and system events.	No exceptions noted.
	Remote Access (OpenVPN)			
		VPN user access is restricted based on the permissions set for each user.	Inspected the VPN user listing, including associated roles, to determine that VPN user access was restricted based on the permissions set for each user.	No exceptions noted.
		The ability to administer VPN access is restricted to user accounts accessible by authorized personnel.	Inquired of the Senior Manager of Information Technology regarding administrative access to the VPN to determine that the ability to administer VPN access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the VPN administrator listing, including associated roles, to determine that the ability to administer VPN access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		VPN users are authenticated via security assertion markup language (SAML) through the identity provider and MFA.	Inquired of the Senior Manager of Information Technology regarding VPN authentication to determine that VPN users were authenticated via SAML through the identity provider and MFA.	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 VPN authentication settings and identity provider settings to determine that VPN users were authenticated via SAML through the identity provider and MFA.	No exceptions noted.
		The VPN is configured to lockout users after a certain number of authentication failures.	Inspected the VPN authentication settings and identity provider settings to determine that the VPN was configured to lockout users after a certain number of authentication failures.	No exceptions noted.
		Subnets and load balancers are utilized to manage and isolate outside access and data from the entity's environment.	Inspected the network diagram, subnets, and load balancers to determine that subnets and load balancers were utilized to manage and isolate outside access and data from the entity's environment.	No exceptions noted.
		The entity secures its environment using a multi-layered defense approach that includes, but is not limited to, a WAF, security groups, an IDS, and antivirus software.	Inspected the WAF settings and host configurations to determine that the entity secured its environment using a multi-layered defense approach that included, but was not limited to, a WAF, security groups, an IDS, and antivirus software.	No exceptions noted.
			Inspected the inbound rules of the security groups for the population of production instances to determine that the entity secured its environment using a multi-layered defense approach that included, but was not limited to, a WAF, security groups, an IDS, and antivirus software.	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 IDS configurations and an example IDS log to determine that the entity secured its environment using a multi-layered defense approach that included, but was not limited to, a WAF, security groups, an IDS, and antivirus software.	No exceptions noted.
			Inspected the antivirus software dashboard console, antivirus software settings, and the listing of devices with the antivirus software installed to determine that the entity secured its environment using a multi-layered defense approach that included, but was not limited to, a WAF, security groups, an IDS, and antivirus software.	No exceptions noted.
		Stored passwords are hashed and salted.	Inspected the code depicting stored passwords were hashed and salted to determine that stored passwords were hashed and salted.	No exceptions noted.
		Data is stored in an encrypted format utilizing encryption keys, server-side encryption, and the advanced encryption standard algorithm.	Inspected the encryption configurations for data at rest to determine that data was stored in an encrypted format utilizing encryption keys, server-side encryption, and the advanced encryption standard algorithm.	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
		Logical access privileges are reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts.	Inquired of the Senior Manager of Information Technology regarding access reviews to determine that logical access privileges were reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts.	No exceptions noted.
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that logical access privileges were reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts.	No exceptions noted.
			Inspected the completed user account review documentation for the in-scope systems for a sample of quarters to determine that logical access privileges were reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts.	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
		Part of this criterion is the responsibility of the subservice organizations. Refer to the ‘Subservice Organizations’ section above for controls managed by the subservice organizations.	Not applicable.	Not applicable.
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.	Policies and procedures are in place that give guidance to personnel on system settings, authentication, access, and security monitoring.	Inspected the information protection policy, the issue tracking policy, and the onboarding, offboarding, user access, and user access review policy to determine that policies and procedures were in place that gave guidance to personnel on system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Senior Manager of Information Technology regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Logical and Physical Access Controls</th></tr>
<tr><th>CC6.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td></td><td>Inspected the user listings for the in-scope systems and the access request documentation for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the user listings for the in-scope systems and the access request documentation for the population of new contractors granted access to the in-scope systems to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Logical access to systems is revoked as a component of the termination process.</td><td>Inquired of the Senior Manager of Information Technology regarding the termination process to determine that logical access to systems was revoked as a component of the termination process.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the onboarding, offboarding, user access, and user access review policy to determine that logical access to systems was revoked as a component of the termination process.</td><td>No exceptions noted.</td></tr>
</table>

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 user listings for the in-scope systems and the access revocation documentation for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the user listings for the in-scope systems and the access revocation documentation for the population of terminated contractors with access to the in-scope systems to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
		Logical access privileges are reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts.	Inquired of the Senior Manager of Information Technology regarding access reviews to determine that logical access privileges were reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts.	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 onboarding, offboarding, user access, and user access review policy to determine that logical access privileges were reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts.	No exceptions noted.
			Inspected the completed user account review documentation for the in-scope systems for a sample of quarters to determine that logical access privileges were reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Vice President and Chief Technology Officer regarding sensitive resources to determine that privileged access to sensitive resources 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
			Inspected the listings of privileged users to Google Workspace, GCP, AWS, the operating system, database, application, and VPN to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Policies and procedures are in place that give guidance to personnel on system settings, authentication, access, and security monitoring.	Inspected the information protection policy, the issue tracking policy, and the onboarding, offboarding, user access, and user access review policy to determine that policies and procedures were in place that gave guidance to personnel on system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Senior Manager of Information Technology regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	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 user listings for the in-scope systems and the access request documentation for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the user listings for the in-scope systems and the access request documentation for the population of new contractors granted access to the in-scope systems to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Senior Manager of Information Technology regarding the termination process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that logical access to systems was revoked as a component of the termination process.	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 user listings for the in-scope systems and the access revocation documentation for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the user listings for the in-scope systems and the access revocation documentation for the population of terminated contractors with access to the in-scope systems to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
		The modification of employee access due to a job change or transfer is authorized and documented.	Inquired of the Vice President and Chief Technology Officer regarding the access modification process to determine that the modification of employee access due to a job change or transfer was authorized and documented.	No exceptions noted.
			Inspected the onboarding, offboarding, user access, and user access review policy to determine that the modification of employee access due to a job change or transfer was authorized and documented.	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 Google Workspace, GCP, AWS, the operating system, database, application, and VPN user listings, and access modification documentation for the population of employees that had a job change or transfer resulting in a change in access permissions to determine that the modification of employee access due to a job change or transfer was authorized and documented.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Vice President and Chief Technology Officer regarding sensitive resources to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to Google Workspace, GCP, AWS, the operating system, database, application, and VPN to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Logical access privileges are reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions are assigned to user accounts.	Inquired of the Senior Manager of Information Technology regarding access reviews to determine that logical access privileges were reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts.	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 onboarding, offboarding, user access, and user access review policy to determine that logical access privileges were reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts.	No exceptions noted.
			Inspected the completed user account review documentation for the in-scope systems for a sample of quarters to determine that logical access privileges were reviewed on a quarterly basis by authorized personnel to help ensure the appropriateness of access credentials and that least privileges required to perform job functions were assigned to user accounts.	No exceptions noted.
	Google Workspace			
		Google Workspace user access is restricted via role-based security privileges defined within the access control system.	Inspected the Google Workspace user listing, including associated role, to determine that Google Workspace user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Logical and Physical Access Controls</th></tr>
<tr><th>CC6.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td colspan="4"><b>GCP</b></td></tr>
<tr><td></td><td></td><td>GCP access and associated user permissions are managed via IAM. Access to GCP is restricted to the administrators.</td><td>Inquired of the Senior Manager of Information Technology regarding access to GCP to determine that GCP access and associated user permissions were managed via IAM, and that access to GCP was restricted to the administrators.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the GCP member listing, including associated roles, to determine that GCP access and associated user permissions were managed via IAM, and that access to GCP was restricted to the administrators.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td colspan="4"><b>AWS</b></td></tr>
<tr><td></td><td></td><td>AWS user access and associated user permissions are managed via IAM.</td><td>Inspected the AWS user listing, including associated groups, to determine that AWS user access and associated user permissions were managed via IAM.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td colspan="4"><b>Operating System (Linux and Windows)</b></td></tr>
<tr><td></td><td></td><td>Operating system users are managed through the defined IAM policies.</td><td>Inquired of the Vice President and Chief Technology Officer regarding the operating system to determine that operating system users were managed via the defined IAM policies.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the operating system user listing, including associated groups, to determine that operating system users were managed via the defined IAM policies.</td><td>No exceptions noted.</td></tr>
</table>

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
	Database (AWS RDS MySQL)			
		Database users are managed and authenticated through the defined IAM policies.	Inquired of the Vice President and Chief Technology Officer regarding the database to determine that database users were managed and authenticated through the defined IAM policies.	No exceptions noted.
			Observed the authentication of a user to the database to determine that database users were managed and authenticated through the defined IAM policies.	No exceptions noted.
			Inspected the AWS user listing, including associated groups and user classes, and the roles and permissions for the database to determine that database users were managed and authenticated through the defined IAM policies.	No exceptions noted.
	Application (OpenSesame)			
		Application user access is restricted via role-based security privileges.	Inspected the application user listing, including associated roles, to determine that application user access was restricted via role-based security privileges.	No exceptions noted.
	Remote Access (OpenVPN)			
		VPN user access is restricted based on the permissions set for each user.	Inspected the VPN user listing, including associated roles, to determine that VPN user access was restricted based on the permissions set for each 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**
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 organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.	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.	Policies and procedures are in place that give guidance to personnel on the retention, handling, classification, and disposal of information and devices.	Inspected the data retention, destruction, backup and relevance policy and the data classification policy to determine that policies and procedures were in place that gave guidance to personnel on the retention, handling, classification, and disposal of information and devices.	No exceptions noted.
		Backups are automatically disposed of after the retention period is met.	Inquired of the Vice President and Chief Technology Officer regarding backups to determine that backups were automatically disposed of after the retention period was met.	No exceptions noted.
			Inspected the backup retention settings and log of snapshots to determine that backups were automatically disposed of after the retention period was met.	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 entity disposes of data in accordance with the retention periods and disposal procedures defined in the data retention, destruction, backup and relevance policy, legal obligations, and various statutes.	Inquired of the Security Analyst regarding data disposal procedures to determine that the entity disposed of data in accordance with the retention periods and disposal procedures defined in the data retention, destruction, backup and relevance policy, legal obligations, and various statutes.	No exceptions noted.
			Inspected the data retention, destruction, backup and relevance policy to determine that the entity disposed of data in accordance with the retention periods and disposal procedures defined in the data retention, destruction, backup and relevance policy, legal obligations, and various statutes.	No exceptions noted.
			Inspected the data disposal ticket for a sample of data disposals to determine that the entity disposed of data in accordance with the retention periods and disposal procedures defined in the data retention, destruction, backup and relevance policy, legal obligations, and various statutes.	Testing of the control activity disclosed that no data disposals occurred during the review period.
		The storage of customer data on removable media is prohibited by policy. Removable storage usage is limited to a read-only state.	Inquired of the Security Analyst regarding data handling to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	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 information protection policy to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	No exceptions noted.
			Inspected the base computer removable storage policy to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.	Not applicable.	Not applicable.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	TLS and HTTPS are used to establish secure connections for defined points of connectivity and data in transit.	Inspected the load balancer listeners, certificates, and the TLS settings to determine that TLS and HTTPS were used to establish secure connections for defined points of connectivity and data in transit.	No exceptions noted.
		VPN user access is restricted based on the permissions set for each user.	Inspected the VPN user listing, including associated roles, to determine that VPN user access was restricted based on the permissions set for each 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**
		VPN users are authenticated via SAML through the identity provider and MFA.	Inquired of the Senior Manager of Information Technology regarding VPN authentication to determine that VPN users were authenticated via SAML through the identity provider and MFA.	No exceptions noted.
			Inspected the VPN authentication settings and identity provider settings to determine that VPN users were authenticated via SAML through the identity provider and MFA.	No exceptions noted.
		A WAF and security groups are in place to filter unauthorized inbound network, application, and API traffic.	Inspected the network diagram to determine that a WAF and security groups were in place to filter unauthorized inbound network, application, and API traffic.	No exceptions noted.
			Inspected the WAF settings and host configurations to determine that a WAF and security groups were in place to filter unauthorized inbound network, application, and API traffic.	No exceptions noted.
			Inspected the inbound rules of the security groups for the population of production instances to determine that a WAF and security groups were in place to filter unauthorized inbound network, application, and API traffic.	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 WAF and security groups are configured to deny any type of connection that is not explicitly authorized by a rule.	Inspected the network diagram to determine that the WAF and security groups were configured to deny any type of connection that was not explicitly authorized by a rule.	No exceptions noted.
			Inspected the WAF settings and host configurations to determine that the WAF and security groups were configured to deny any type of connection that was not explicitly authorized by a rule.	No exceptions noted.
			Inspected the inbound rules of the security groups for the population of production instances to determine that the WAF and security groups were configured to deny any type of connection that was not explicitly authorized by a rule.	No exceptions noted.
		An IDS is utilized to analyze AWS events and report possible or actual security breaches.	Inspected the IDS configurations and an example IDS log to determine that an IDS was utilized to analyze AWS events and report possible or actual security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS alert rules, SNS topic, and an example alert to determine that the IDS was configured to notify personnel upon intrusion detection.	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**
		Antivirus software is installed on servers and workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console, antivirus software settings, and the listing of devices with the antivirus software installed to determine that antivirus software was installed on servers and workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new security updates are available and weekly for product updates.	Inspected the antivirus software settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new security updates were available and weekly for product updates.	No exceptions noted.
		Scheduled scans are configured to run daily for workstations and weekly for servers. Runtime protection and real-time scanning are enabled for workstations and servers.	Inspected the antivirus software settings to determine that scheduled scans were configured to run daily for workstations and weekly for servers, and that runtime protection and real-time scanning were enabled for workstations and servers.	No exceptions noted.
		Data is stored in an encrypted format utilizing encryption keys, server-side encryption, and the advanced encryption standard algorithm.	Inspected the encryption configurations for data at rest to determine that data was stored in an encrypted format utilizing encryption keys, server-side encryption, and the advanced encryption standard algorithm.	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
		Subnets and load balancers are utilized to manage and isolate outside access and data from the entity's environment.	Inspected the network diagram, subnets, and load balancers to determine that subnets and load balancers were utilized to manage and isolate outside access and data from the entity's environment.	No exceptions noted.
		The storage of customer data on removable media is prohibited by policy. Removable storage usage is limited to a read-only state.	Inquired of the Security Analyst regarding data handling to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	No exceptions noted.
			Inspected the information protection policy to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	No exceptions noted.
			Inspected the base computer removable storage policy to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	No exceptions noted.
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.	TLS and HTTPS are used to establish secure connections for defined points of connectivity and data in transit.	Inspected the load balancer listeners, certificates, and the TLS settings to determine that TLS and HTTPS were used to establish secure connections for defined points of connectivity and data in transit.	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 WAF and security groups are in place to filter unauthorized inbound network, application, and API traffic.	Inspected the network diagram to determine that a WAF and security groups were in place to filter unauthorized inbound network, application, and API traffic.	No exceptions noted.
			Inspected the WAF settings and host configurations to determine that a WAF and security groups were in place to filter unauthorized inbound network, application, and API traffic.	No exceptions noted.
			Inspected the inbound rules of the security groups for the population of production instances to determine that a WAF and security groups were in place to filter unauthorized inbound network, application, and API traffic.	No exceptions noted.
		The WAF and security groups are configured to deny any type of connection that is not explicitly authorized by a rule.	Inspected the network diagram to determine that the WAF and security groups were configured to deny any type of connection that was not explicitly authorized by a rule.	No exceptions noted.
			Inspected the WAF settings and host configurations to determine that the WAF and security groups were configured to deny any type of connection that was not explicitly authorized by a rule.	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 inbound rules of the security groups for the population of production instances to determine that the WAF and security groups were configured to deny any type of connection that was not explicitly authorized by a rule.	No exceptions noted.
		An IDS is utilized to analyze AWS events and report possible or actual security breaches.	Inspected the IDS configurations and an example IDS log to determine that an IDS was utilized to analyze AWS events and report possible or actual security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS alert rules, SNS topic, and an example alert to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Data is stored in an encrypted format utilizing encryption keys, server-side encryption, and the advanced encryption standard algorithm.	Inspected the encryption configurations for data at rest to determine that data was stored in an encrypted format utilizing encryption keys, server-side encryption, and the advanced encryption standard algorithm.	No exceptions noted.
		The storage of customer data on removable media is prohibited by policy. Removable storage usage is limited to a read-only state.	Inquired of the Security Analyst regarding data handling to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	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 information protection policy to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	No exceptions noted.
			Inspected the base computer removable storage policy to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	No exceptions noted.
		Mobile devices are centrally managed through a mobile device manager to allow for remote management of devices.	Inspected the mobile device manager settings and listing of devices managed to determine that mobile devices were centrally managed through a mobile device manager to allow for remote management of devices.	No exceptions noted.
		DLP software is utilized to prevent the misuse and loss of sensitive data.	Inspected the DLP software settings and data protection rules to determine that DLP software was utilized to prevent the misuse and loss of sensitive data.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.	Not applicable.	Not applicable.

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**
CC6.8	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 ability to install applications and software are restricted to authorized personnel.	Inquired of the Vice President and Chief Technology Officer regarding the installation of applications and software to determine that the ability to install applications and software were restricted to authorized personnel.	No exceptions noted.
			Inspected the prompt demonstrating the downloading of unauthorized applications and software were restricted to system administrators and unapproved applications and software were unable to be downloaded to determine that the ability to install applications and software were restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of individuals with the ability to download applications and software to determine that the ability to install applications and software were restricted to authorized personnel.	No exceptions noted.
		A change management policy is in place to guide personnel in the change management process, including emergency changes.	Inspected the change management policy to determine that a change management policy was in place to guide personnel in the change management process, including emergency changes.	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 ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Vice President and Chief Technology Officer regarding the ability to migrate changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
			Inspected the listing of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
		FIM software is in place to detect activity which includes, but is not limited to, file changes, admin activity, process activity, and security group activity.	Inspected the FIM rules to determine that FIM software was in place to detect activity which included, but was not limited to, file changes, admin activity, process activity, and security group activity.	No exceptions noted.
		The FIM software is configured to notify IT personnel when threats exceeding a severity are triggered, in addition to the daily activity reports.	Inspected the FIM notification settings and an example FIM alert to determine that the FIM software was configured to notify IT personnel when threats exceeding a severity were triggered, in addition to the daily activity reports.	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**
		Antivirus software is installed on servers and workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console, antivirus software settings, and the listing of devices with the antivirus software installed to determine that antivirus software was installed on servers and workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new security updates are available and weekly for product updates.	Inspected the antivirus software settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new security updates were available and weekly for product updates.	No exceptions noted.
		Scheduled scans are configured to run daily for workstations and weekly for servers. Runtime protection and real-time scanning are enabled for workstations and servers.	Inspected the antivirus software settings to determine that scheduled scans were configured to run daily for workstations and weekly for servers, and that runtime protection and real-time scanning were enabled for workstations and servers.	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.	Configuration standards are outlined within the network and host configuration policy.	Inspected the network and host configuration policy to determine that configuration standards were outlined within the network and host configuration policy.	No exceptions noted.
		Policies and procedures are in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information protection policy, the incident response policy, and the issue tracking policy to determine that policies and procedures were in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		System logging and monitoring software is used to collect data from system infrastructure components and endpoints, and to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity. Alerts are sent to personnel when certain alarms are triggered.	Inspected the monitoring software configurations, rules, SNS topics, alert settings, integrations, and example alerts to determine that system logging and monitoring software was used to collect data from system infrastructure components and endpoints, and to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity, and that alerts were sent to personnel when certain alarms were triggered.	No exceptions noted.
		A WAF and security groups are in place to filter unauthorized inbound network, application, and API traffic.	Inspected the network diagram to determine that a WAF and security groups were in place to filter unauthorized inbound network, application, and API traffic.	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 settings and host configurations to determine that a WAF and security groups were in place to filter unauthorized inbound network, application, and API traffic.	No exceptions noted.
			Inspected the inbound rules of the security groups for the population of production instances to determine that a WAF and security groups were in place to filter unauthorized inbound network, application, and API traffic.	No exceptions noted.
		The WAF and security groups are configured to deny any type of connection that is not explicitly authorized by a rule.	Inspected the network diagram to determine that the WAF and security groups were configured to deny any type of connection that was not explicitly authorized by a rule.	No exceptions noted.
			Inspected the WAF settings and host configurations to determine that the WAF and security groups were configured to deny any type of connection that was not explicitly authorized by a rule.	No exceptions noted.
			Inspected the inbound rules of the security groups for the population of production instances to determine that the WAF and security groups were configured to deny any type of connection that was not explicitly authorized by a rule.	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
		An IDS is utilized to analyze AWS events and report possible or actual security breaches.	Inspected the IDS configurations and an example IDS log to determine that an IDS was utilized to analyze AWS events and report possible or actual security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS alert rules, SNS topic, and an example alert to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		FIM software is in place to detect activity which includes, but is not limited to, file changes, admin activity, process activity, and security group activity.	Inspected the FIM rules to determine that FIM software was in place to detect activity which included, but was not limited to, file changes, admin activity, process activity, and security group activity.	No exceptions noted.
		The FIM software is configured to notify IT personnel when threats exceeding a severity are triggered, in addition to the daily activity reports.	Inspected the FIM notification settings and an example FIM alert to determine that the FIM software was configured to notify IT personnel when threats exceeding a severity were triggered, in addition to the daily activity reports.	No exceptions noted.
		A third-party vulnerability scanning tool is utilized to continuously scan assets for vulnerabilities.	Inquired of the Security Analyst regarding vulnerability scanning to determine that a third-party vulnerability scanning tool was utilized to continuously scan assets for vulnerabilities.	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 vulnerability scanning tool schedule, scan activity report, and an example executive summary report to determine that a third-party vulnerability scanning tool was utilized to continuously scan assets for vulnerabilities.	No exceptions noted.
		A third-party performs a penetration test annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test report to determine that a third-party performed a penetration test annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		The storage of customer data on removable media is prohibited by policy. Removable storage usage is limited to a read-only state.	Inquired of the Security Analyst regarding data handling to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	No exceptions noted.
			Inspected the information protection policy to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	No exceptions noted.
			Inspected the base computer removable storage policy to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">System Operations</th></tr>
<tr><th>CC7.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td>CC7.2</td><td>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.</td><td>Policies and procedures are in place that include defined responsibilities, communication protocols, and give guidance to personnel over the investigation, evaluation, documentation, and resolution of an incident. The policies and procedures are made available to personnel and reviewed at least annually.</td><td>Inspected the information protection policy, the incident response policy, the issue tracking policy, and the entity's intranet site to determine that policies and procedures were in place that included defined responsibilities, communication protocols, and gave guidance to personnel over the investigation, evaluation, documentation, and resolution of an incident, and that the policies and procedures were made available to personnel and reviewed at least annually.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Policies and procedures are in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.</td><td>Inspected the information protection policy, the incident response policy, and the issue tracking policy to determine that policies and procedures were in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.</td><td>No exceptions noted.</td></tr>
</table>

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
		System logging and monitoring software is used to collect data from system infrastructure components and endpoints, and to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity. Alerts are sent to personnel when certain alarms are triggered.	Inspected the monitoring software configurations, rules, SNS topics, alert settings, integrations, and example alerts to determine that system logging and monitoring software was used to collect data from system infrastructure components and endpoints, and to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity, and that alerts were sent to personnel when certain alarms were triggered.	No exceptions noted.
		A WAF and security groups are in place to filter unauthorized inbound network, application, and API traffic.	Inspected the network diagram to determine that a WAF and security groups were in place to filter unauthorized inbound network, application, and API traffic.	No exceptions noted.
			Inspected the WAF settings and host configurations to determine that a WAF and security groups were in place to filter unauthorized inbound network, application, and API traffic.	No exceptions noted.
			Inspected the inbound rules of the security groups for the population of production instances to determine that a WAF and security groups were in place to filter unauthorized inbound network, application, and API traffic.	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 WAF and security groups are configured to deny any type of connection that is not explicitly authorized by a rule.	Inspected the network diagram to determine that the WAF and security groups were configured to deny any type of connection that was not explicitly authorized by a rule.	No exceptions noted.
			Inspected the WAF settings and host configurations to determine that the WAF and security groups were configured to deny any type of connection that was not explicitly authorized by a rule.	No exceptions noted.
			Inspected the inbound rules of the security groups for the population of production instances to determine that the WAF and security groups were configured to deny any type of connection that was not explicitly authorized by a rule.	No exceptions noted.
		An IDS is utilized to analyze AWS events and report possible or actual security breaches.	Inspected the IDS configurations and an example IDS log to determine that an IDS was utilized to analyze AWS events and report possible or actual security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS alert rules, SNS topic, and an example alert to determine that the IDS was configured to notify personnel upon intrusion detection.	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**
		FIM software is in place to detect activity which includes, but is not limited to, file changes, admin activity, process activity, and security group activity.	Inspected the FIM rules to determine that FIM software was in place to detect activity which included, but was not limited to, file changes, admin activity, process activity, and security group activity.	No exceptions noted.
		The FIM software is configured to notify IT personnel when threats exceeding a severity are triggered, in addition to the daily activity reports.	Inspected the FIM notification settings and an example FIM alert to determine that the FIM software was configured to notify IT personnel when threats exceeding a severity were triggered, in addition to the daily activity reports.	No exceptions noted.
		Antivirus software is installed on servers and workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console, antivirus software settings, and the listing of devices with the antivirus software installed to determine that antivirus software was installed on servers and workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new security updates are available and weekly for product updates.	Inspected the antivirus software settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new security updates were available and weekly for product updates.	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
		Scheduled scans are configured to run daily for workstations and weekly for servers. Runtime protection and real-time scanning are enabled for workstations and servers.	Inspected the antivirus software settings to determine that scheduled scans were configured to run daily for workstations and weekly for servers, and that runtime protection and real-time scanning were enabled for workstations and servers.	No exceptions noted.
		The storage of customer data on removable media is prohibited by policy. Removable storage usage is limited to a read-only state.	Inquired of the Security Analyst regarding data handling to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	No exceptions noted.
			Inspected the information protection policy to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	No exceptions noted.
			Inspected the base computer removable storage policy to determine that the storage of customer data on removable media was prohibited by policy, and that removable storage usage was limited to a read-only state.	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**
	AWS			
		AWS audit logging is configured to log various actions across the AWS infrastructure, including any API and management console activity.	Inspected the AWS trails and an example AWS event history log to determine that AWS audit logging was configured to log various actions across the AWS infrastructure, including any API and management console activity.	No exceptions noted.
	Database (AWS RDS MySQL)			
		The database is configured to log server activity, which includes when clients connect, disconnect, and activity performed while connected.	Inspected the database audit logging configurations and an example database audit log to determine that the database was configured to log server activity, which included when clients connected, disconnected, and activity performed while connected.	No exceptions noted.
	Application (OpenSesame)			
		Logging is configured for the application to log any user activity and system events.	Inspected the application audit logging configurations and an example application log to determine that logging was configured for the application to log any user activity and system events.	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 Security team meets on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	Inquired of the Vice President and Chief Technology Officer regarding the Security team to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the issue tracking policy to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the Security team meeting minutes for a sample of months to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organizations. Refer to the ‘Subservice Organizations’ section above for controls managed by the subservice organizations.	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.	Policies and procedures are in place that include defined responsibilities, communication protocols, and give guidance to personnel over the investigation, evaluation, documentation, and resolution of an incident. The policies and procedures are made available to personnel and reviewed at least annually.	Inspected the information protection policy, the incident response policy, the issue tracking policy, and the entity's intranet site to determine that policies and procedures were in place that included defined responsibilities, communication protocols, and gave guidance to personnel over the investigation, evaluation, documentation, and resolution of an incident, and that the policies and procedures were made available to personnel and reviewed at least annually.	No exceptions noted.
		The incident response policy defines the classification of incidents based on severity, which determines the appropriate response strategy.	Inspected the incident response policy to determine that the incident response policy defined the classification of incidents based on severity, which determined the appropriate response strategy.	No exceptions noted.
		Identified incidents are reviewed, monitored, and investigated by the Security team.	Inquired of the Vice President and Chief Technology Officer regarding security incidents to determine that identified incidents were reviewed, monitored, and investigated by the Security team.	No exceptions noted.
			Inspected the incident response policy to determine that identified incidents were reviewed, monitored, and investigated by the Security team.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">System Operations</th></tr>
<tr><th>CC7.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td></td><td>Inspected the incident handling documentation for a sample of incidents to determine that identified incidents were reviewed, monitored, and investigated by the Security team.</td><td>Testing of the control activity disclosed that no security incidents occurred during the review period.</td></tr>
<tr><td></td><td></td><td>Incident handling, including remediation, is documented and tracked in a ticket and/or an incident response checklist.</td><td>Inquired of the Vice President and Chief Technology Officer regarding security incidents to determine that incident handling, including remediation, was documented and tracked in a ticket and/or an incident response checklist.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the incident response policy and the issue tracking policy to determine that incident handling, including remediation, was documented and tracked in a ticket and/or an incident response checklist.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the incident handling documentation for a sample of incidents to determine that incident handling, including remediation, was documented and tracked in a ticket and/or an incident response checklist.</td><td>Testing of the control activity disclosed that no security incidents occurred during the review period.</td></tr>
</table>

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
		Following an incident, a post-mortem and root cause analysis are performed to evaluate the incident and discuss possible procedures to implement to prevent future similar incidents from reoccurring and potential updates to policies, controls, or security measures.	Inquired of the Vice President and Chief Technology Officer regarding security incidents to determine that following an incident, a post-mortem and root cause analysis were performed to evaluate the incident and discuss possible procedures to implement to prevent future similar incidents from reoccurring and potential updates to policies, controls, or security measures.	No exceptions noted.
			Inspected the incident response policy to determine that following an incident, a post-mortem and root cause analysis were performed to evaluate the incident and discuss possible procedures to implement to prevent future similar incidents from reoccurring and potential updates to policies, controls, or security measures.	No exceptions noted.
			Inspected the incident handling documentation for a sample of incidents to determine that following an incident, a post-mortem and root cause analysis were performed to evaluate the incident and discuss possible procedures to implement to prevent future similar incidents from reoccurring and potential updates to policies, controls, or security measures.	Testing of the control activity disclosed that no security incidents 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 Security team meets on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	Inquired of the Vice President and Chief Technology Officer regarding the Security team to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the issue tracking policy to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the Security team meeting minutes for a sample of months to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	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**
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Policies and procedures are in place that include defined responsibilities, communication protocols, and give guidance to personnel over the investigation, evaluation, documentation, and resolution of an incident. The policies and procedures are made available to personnel and reviewed at least annually.	Inspected the information protection policy, the incident response policy, the issue tracking policy, and the entity's intranet site to determine that policies and procedures were in place that included defined responsibilities, communication protocols, and gave guidance to personnel over the investigation, evaluation, documentation, and resolution of an incident, and that the policies and procedures were made available to personnel and reviewed at least annually.	No exceptions noted.
		The incident response policy defines the classification of incidents based on severity, which determines the appropriate response strategy.	Inspected the incident response policy to determine that the incident response policy defined the classification of incidents based on severity, which determined the appropriate response strategy.	No exceptions noted.
		Identified incidents are reviewed, monitored, and investigated by the Security team.	Inquired of the Vice President and Chief Technology Officer regarding security incidents to determine that identified incidents were reviewed, monitored, and investigated by the Security team.	No exceptions noted.
			Inspected the incident response policy to determine that identified incidents were reviewed, monitored, and investigated by the Security team.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">System Operations</th></tr>
<tr><th>CC7.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td></td><td>Inspected the incident handling documentation for a sample of incidents to determine that identified incidents were reviewed, monitored, and investigated by the Security team.</td><td>Testing of the control activity disclosed that no security incidents occurred during the review period.</td></tr>
<tr><td></td><td></td><td>Incident handling, including remediation, is documented and tracked in a ticket and/or an incident response checklist.</td><td>Inquired of the Vice President and Chief Technology Officer regarding security incidents to determine that incident handling, including remediation, was documented and tracked in a ticket and/or an incident response checklist.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the incident response policy and the issue tracking policy to determine that incident handling, including remediation, was documented and tracked in a ticket and/or an incident response checklist.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the incident handling documentation for a sample of incidents to determine that incident handling, including remediation, was documented and tracked in a ticket and/or an incident response checklist.</td><td>Testing of the control activity disclosed that no security incidents occurred during the review period.</td></tr>
</table>

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**
		Following an incident, a post-mortem and root cause analysis are performed to evaluate the incident and discuss possible procedures to implement to prevent future similar incidents from reoccurring and potential updates to policies, controls, or security measures.	Inquired of the Vice President and Chief Technology Officer regarding security incidents to determine that following an incident, a post-mortem and root cause analysis were performed to evaluate the incident and discuss possible procedures to implement to prevent future similar incidents from reoccurring and potential updates to policies, controls, or security measures.	No exceptions noted.
			Inspected the incident response policy to determine that following an incident, a post-mortem and root cause analysis were performed to evaluate the incident and discuss possible procedures to implement to prevent future similar incidents from reoccurring and potential updates to policies, controls, or security measures.	No exceptions noted.
			Inspected the incident handling documentation for a sample of incidents to determine that following an incident, a post-mortem and root cause analysis were performed to evaluate the incident and discuss possible procedures to implement to prevent future similar incidents from reoccurring and potential updates to policies, controls, or security measures.	Testing of the control activity disclosed that no security incidents 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 Security team meets on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	Inquired of the Vice President and Chief Technology Officer regarding the Security team to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the issue tracking policy to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the Security team meeting minutes for a sample of months to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
		The incident response policy is tested on an annual basis to evaluate overall incident response effectiveness. The incident response policy is updated based on test results, as applicable.	Inquired of the Vice President and Chief Technology Officer regarding security incidents to determine that the incident response policy was tested on an annual basis to evaluate overall incident response effectiveness, and that the incident response policy was updated based on test results, as applicable.	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 policy to determine that the incident response policy was tested on an annual basis to evaluate overall incident response effectiveness, and that the incident response policy was updated based on test results, as applicable.	No exceptions noted.
			Inspected the incident response test meeting documentation and meeting invite to determine that the incident response policy was tested on an annual basis to evaluate overall incident response effectiveness, and that the incident response policy was updated based on test results, as applicable.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Change management requests are opened for incidents that require permanent fixes.	Inquired of the Vice President and Chief Technology Officer regarding security incidents to determine that change management requests were opened for incidents that required permanent fixes.	No exceptions noted.
			Inspected the incident response policy and the change management policy to determine that change management requests were opened for incidents that required permanent fixes.	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 handling documentation and change management documentation for a sample of incidents to determine that change management requests were opened for incidents that required permanent fixes.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		Following an incident, a post-mortem and root cause analysis are performed to evaluate the incident and discuss possible procedures to implement to prevent future similar incidents from reoccurring and potential updates to policies, controls, or security measures.	Inquired of the Vice President and Chief Technology Officer regarding security incidents to determine that following an incident, a post-mortem and root cause analysis were performed to evaluate the incident and discuss possible procedures to implement to prevent future similar incidents from reoccurring and potential updates to policies, controls, or security measures.	No exceptions noted.
			Inspected the incident response policy to determine that following an incident, a post-mortem and root cause analysis were performed to evaluate the incident and discuss possible procedures to implement to prevent future similar incidents from reoccurring and potential updates to policies, controls, or security measures.	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 handling documentation for a sample of incidents to determine that following an incident, a post-mortem and root cause analysis were performed to evaluate the incident and discuss possible procedures to implement to prevent future similar incidents from reoccurring and potential updates to policies, controls, or security measures.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		The Security team meets on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	Inquired of the Vice President and Chief Technology Officer regarding the Security team to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
			Inspected the issue tracking policy to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	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 Security team meeting minutes for a sample of months to determine that the Security team met on a quarterly basis to review internal compliance activities, ongoing security initiatives, issues, risks, controls, and assessments performed.	No exceptions noted.
		The incident response policy is tested on an annual basis to evaluate overall incident response effectiveness. The incident response policy is updated based on test results, as applicable.	Inquired of the Vice President and Chief Technology Officer regarding security incidents to determine that the incident response policy was tested on an annual basis to evaluate overall incident response effectiveness, and that the incident response policy was updated based on test results, as applicable.	No exceptions noted.
			Inspected the incident response policy to determine that the incident response policy was tested on an annual basis to evaluate overall incident response effectiveness, and that the incident response policy was updated based on test results, as applicable.	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 test meeting documentation and meeting invite to determine that the incident response policy was tested on an annual basis to evaluate overall incident response effectiveness, and that the incident response policy was updated based on test results, as applicable.	No exceptions noted.
		A backup restoration test is performed on an annual basis.	Inquired of the Security Analyst regarding restore testing to determine that a backup restoration test was performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test results and restore test script to determine that a backup restoration test was performed on an annual basis.	No exceptions noted.
		A disaster recovery policy and a business continuity and emergency communication policy are in place to give guidance to personnel on how to recover from a disaster and ensure the timely resumption of essential operations.	Inspected the disaster recovery policy and the business continuity and emergency communication policy to determine that a disaster recovery policy and a business continuity and emergency communication policy were in place to give guidance to personnel on how to recover from a disaster and ensure the timely resumption of essential operations.	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 disaster recovery policy and business continuity and emergency communication policy are tested at least annually. Updates to the policies are made based on test results, as applicable.	Inquired of the Senior Manager of Information Technology regarding disasters to determine that the disaster recovery policy and business continuity and emergency communication policy were tested at least annually, and that updates to the policies were made based on test results, as applicable.	No exceptions noted.
			Inspected the disaster recovery policy and the business continuity and emergency communication policy to determine that the disaster recovery policy and business continuity and emergency communication policy were tested at least annually, and that updates to the policies were made based on test results, as applicable.	No exceptions noted.
			Inspected the completed disaster recovery test documentation to determine that the disaster recovery policy and business continuity and emergency communication policy were tested at least annually, and that updates to the policies were made based on test results, as applicable.	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.	A change management policy is in place to guide personnel in the change management process, including emergency changes.	Inspected the change management policy to determine that a change management policy was in place to guide personnel in the change management process, including emergency changes.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Engineering and Product leadership - Maintain change workflow • Engineering Team - Change communications • Security Team - Approval of changes and verification	Inspected the change management policy to determine that the change management process had defined the following roles and assignments: • Engineering and Product leadership - Maintain change workflow • Engineering Team - Change communications • Security Team - Approval of changes and verification	No exceptions noted.
		System changes are documented in a ticket and PR and tracked through the change process to implementation.	Inquired of the Vice President and Chief Technology Officer regarding changes to determine that system changes were documented in a ticket and PR and tracked through the change process to implementation.	No exceptions noted.
			Inspected the change management policy to determine that system changes were documented in a ticket and PR and tracked through the change process to implementation.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Change Management</th></tr>
<tr><th>CC8.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td></td><td>Inspected the ticket and PR, as applicable, for a sample of infrastructure changes to determine that system changes were documented in a ticket and PR and tracked through the change process to implementation.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the ticket and PR, as applicable, for a sample of application changes to determine that system changes were documented in a ticket and PR and tracked through the change process to implementation.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Development and staging environments are logically separated from the production environment.</td><td>Inspected the separate development, staging, and production environments to determine that development and staging environments were logically separated from the production environment.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>System changes are tested through a CI/CD pipeline that runs automated tests and security checks prior to deployment.</td><td>Inquired of the Vice President and Chief Technology Officer regarding changes to determine that system changes were tested through a CI/CD pipeline that ran automated tests and security checks prior to deployment.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the change management policy to determine that system changes were tested through a CI/CD pipeline that ran automated tests and security checks prior to deployment.</td><td>No exceptions noted.</td></tr>
</table>

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**
			Inspected the branch protection rule settings to determine that system changes were tested through a CI/CD pipeline that ran automated tests and security checks prior to deployment.	No exceptions noted.
			Inspected the ticket and PR, as applicable, for a sample of infrastructure changes to determine that system changes were tested through a CI/CD pipeline that ran automated tests and security checks prior to deployment.	No exceptions noted.
			Inspected the ticket and PR, as applicable, for a sample of application changes to determine that system changes were tested through a CI/CD pipeline that ran automated tests and security checks prior to deployment.	No exceptions noted.
		A non-author engineer is systematically required to perform a peer review of the PR prior to deploying into the production environment.	Inquired of the Vice President and Chief Technology Officer regarding changes to determine that a non-author engineer was systematically required to perform a peer review of the PR prior to deploying into the production environment.	No exceptions noted.
			Inspected the change management policy to determine that a non-author engineer was systematically required to perform a peer review of the PR prior to deploying into the production environment.	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
			Inspected the branch protection rule settings to determine that a non-author engineer was systematically required to perform a peer review of the PR prior to deploying into the production environment.	No exceptions noted.
			Inspected the ticket and PR, as applicable, for a sample of infrastructure changes to determine that a non-author engineer was systematically required to perform a peer review of the PR prior to deploying into the production environment.	No exceptions noted.
			Inspected the ticket and PR, as applicable, for a sample of application changes to determine that a non-author engineer was systematically required to perform a peer review of the PR prior to deploying into the production environment.	No exceptions noted.
		The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Vice President and Chief Technology Officer regarding the ability to migrate changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	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**
			Inspected the listing of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
		Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.	Inspected the source code repository to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed.	No exceptions noted.
		FIM software is in place to detect activity which includes, but is not limited to, file changes, admin activity, process activity, and security group activity.	Inspected the FIM rules to determine that FIM software was in place to detect activity which included, but was not limited to, file changes, admin activity, process activity, and security group activity.	No exceptions noted.
		The FIM software is configured to notify IT personnel when threats exceeding a severity are triggered, in addition to the daily activity reports.	Inspected the FIM notification settings and an example FIM alert to determine that the FIM software was configured to notify IT personnel when threats exceeding a severity were triggered, in addition to the daily activity reports.	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
		Monitoring is configured so that the Engineering Managers receive a notification in the event a change is released to production.	Inquired of the Vice President and Chief Technology Officer regarding changes to determine that monitoring was configured so that the Engineering Managers received a notification in the event a change was released to production.	No exceptions noted.
			Inspected the deployment tool configurations, event rules, and an example alert to determine that monitoring was configured so that the Engineering Managers received a notification in the event a change was released to production.	No exceptions noted.
		System changes are communicated to both impacted internal and external users.	Inquired of the Vice President and Chief Technology Officer regarding changes to determine that system changes were communicated to both impacted internal and external users.	No exceptions noted.
			Inspected the internal channel utilized to communicate releases, an example releases notes alert, and an example set of release notes to determine that system changes were communicated to both impacted internal and external users.	No exceptions noted.
			Inspected the release notes channel on the entity's externally-facing website to determine that system changes were communicated to both impacted internal and external users.	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 risk management policy and issue tracking policy contain procedures around the risk management process to guide personnel in identifying threats and vulnerabilities, evaluating and addressing risks, defining specified risk tolerances, and risk mitigation.	Inspected the risk management policy and issue tracking policy to determine that the risk management policy and issue tracking policy contained procedures around the risk management process to guide personnel in identifying threats and vulnerabilities, evaluating and addressing risks, defining specified risk tolerances, and risk mitigation.	No exceptions noted.
		The entity utilizes a GRC tool to manage internal risk and compliance activities and risks associated with external parties. At least annually, personnel with risk management responsibilities assess changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives in the GRC tool.	Inquired of the Vice President and Chief Technology Officer regarding risk management procedures to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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**
			Observed the workflows and risk management processes of the GRC tool to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	No exceptions noted.
			Inspected the completed risk assessment report to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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
		Risks identified as part of the risk management process are evaluated by determining the initial impact and likelihood of the risk as if no controls are in place to establish the maximum risk, determining the controls and mitigating factors in place, then reevaluating the risk impact and likelihood with controls and mitigating factors present to establish the overall residual risk level.	Inquired of the Vice President and Chief Technology Officer regarding risk management procedures to determine that risks identified as part of the risk management process were evaluated by determining the initial impact and likelihood of the risk as if no controls were in place to establish the maximum risk, determining the controls and mitigating factors in place, then reevaluating the risk impact and likelihood with controls and mitigating factors present to establish the overall residual risk level.	No exceptions noted.
			Observed the workflows and risk management processes of the GRC tool to determine that risks identified as part of the risk management process were evaluated by determining the initial impact and likelihood of the risk as if no controls were in place to establish the maximum risk, determining the controls and mitigating factors in place, then reevaluating the risk impact and likelihood with controls and mitigating factors present to establish the overall residual risk level.	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
			Inspected the completed risk assessment report to determine that risks identified as part of the risk management process were evaluated by determining the initial impact and likelihood of the risk as if no controls were in place to establish the maximum risk, determining the controls and mitigating factors in place, then reevaluating the risk impact and likelihood with controls and mitigating factors present to establish the overall residual risk level.	No exceptions noted.
		Issues identified from the various evaluations performed are tracked by management through the GRC tool or ticketing system to ensure they are addressed in a timely manner.	Inquired of the Vice President and Chief Technology Officer regarding issue management to determine that issues identified from the various evaluations performed were tracked by management through the GRC tool or ticketing system to ensure they were addressed in a timely manner.	No exceptions noted.
			Inspected the issue tracking policy to determine that issues identified from the various evaluations performed were tracked by management through the GRC tool or ticketing system to ensure they were addressed in a timely manner.	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
			Inspected the issues board within the GRC tool and ticketing system to determine that issues identified from the various evaluations performed were tracked by management through the GRC tool or ticketing system to ensure they were addressed in a timely manner.	No exceptions noted.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the cyber liability certificate of insurance to determine that the entity had purchased insurance to offset the financial loss that could have resulted from a critical security incident or exploitation of a vulnerability.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	A vendor risk management policy is in place and outlines the procedures to be followed when assessing the security posture of critical vendors.	Inspected the vendor risk management policy to determine that a vendor risk management policy was in place and outlined the procedures to be followed when assessing the security posture of critical vendors.	No exceptions noted.
		The entity evaluates the competencies and experience of third-party vendors prior to working with them.	Inquired of the Security Analyst regarding the third-party vendor risk assessment process to determine that the entity evaluated the competencies and experience of third-party vendors prior to working with them.	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
			Inspected the vendor risk management policy to determine that the entity evaluated the competencies and experience of third-party vendors prior to working with them.	No exceptions noted.
			Inspected the vendor risk analysis for a sample of new third-party vendors to determine that the entity evaluated the competencies and experience of third-party vendors prior to working with them.	Testing of the control activity disclosed that no new third-party vendors were onboarded during the review period.
		Management performs annual due diligence procedures on third-party vendors who are classified as a sub-processor. Monitoring procedures include maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	Inquired of the Security Analyst regarding the third-party vendor risk assessment process to determine that management performed annual due diligence procedures on third-party vendors who were classified as a sub-processor, and that monitoring procedures included maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	No exceptions noted.
			Inspected the vendor risk management policy to determine that management performed annual due diligence procedures on third-party vendors who were classified as a sub-processor, and that monitoring procedures included maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	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
			Inspected the listing of third-party sub-processors, attestation report, and vendor attestation report review meeting minutes for a sample of third-party vendors to determine that management performed annual due diligence procedures on third-party vendors who were classified as a sub-processor, and that monitoring procedures included maintaining an inventory of third-party vendors and assessing applicable SOC reports for the third-party vendors.	No exceptions noted.
		The entity utilizes a GRC tool to manage internal risk and compliance activities and risks associated with external parties. At least annually, personnel with risk management responsibilities assess changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives in the GRC tool.	Inquired of the Vice President and Chief Technology Officer regarding risk management procedures to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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
			Observed the workflows and risk management processes of the GRC tool to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	No exceptions noted.
			Inspected the completed risk assessment report to determine that the entity utilized a GRC tool to manage internal risk and compliance activities and risks associated with external parties, and that at least annually, personnel with risk management responsibilities assessed changes to business objectives, commitments and requirements, internal operations and controls, fraud risks, external parties, and external factors that threatened the achievement of business objectives, and updated the potential threats to system objectives in the GRC tool.	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
		Third-party agreements outline and communicate the system commitments, requirements, terms, conditions and responsibilities of third-party vendors.	Inspected the agreement for a sample of third-party vendors to determine that third-party agreements outlined and communicated the system commitments, requirements, terms, conditions and responsibilities of third-party vendors.	No exceptions noted.
		Procedures are in place that outline the process of handling issues with vendors, such as non-compliance.	Inspected the vendor risk management policy to determine that procedures were in place that outlined the process of handling issues with vendors, such as non-compliance.	No exceptions noted.