A-LIGN

A-LIGN.com

Type 2 SOC 2

Prepared for:
Learning Technologies
Acquisition Corporation

Year:
2026

ltg learning technologies group

REPORT ON LEARNING TECHNOLOGIES ACQUISITION CORPORATION'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

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

April 1, 2025 to March 31, 2026

Table of Contents

SECTION 1

ASSERTION OF LEARNING TECHNOLOGIES ACQUISITION CORPORATION MANAGEMENT

ASSERTION OF LEARNING TECHNOLOGIES ACQUISITION CORPORATION MANAGEMENT

May 7, 2026

We have prepared the accompanying description of Learning Technologies Acquisition Corporation's ('LTG' or 'the Company') SaaS Offering Services System titled "Learning Technologies Acquisition Corporation's Description of Its SaaS Offering Services System throughout the period April 1, 2025 to March 31, 2026" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the SaaS Offering Services System that may be useful when assessing the risks arising from interactions with LTG's system, particularly information about system controls that LTG has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

LTG uses Amazon Web Services ('AWS') to provide cloud hosting services, Centersquare and Digital Realty Trust, Inc ('Digital Realty') to provide data center hosting and customer 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 LTG, to achieve LTG's service commitments and system requirements based on the applicable trust services criteria. The description presents LTG's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of LTG'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 LTG, to achieve LTG's service commitments and system requirements based on the applicable trust services criteria. The description presents LTG's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of LTG's controls.

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

a. the description presents LTG's SaaS Offering Services System that was designed and implemented throughout the period April 1, 2025 to March 31, 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period April 1, 2025 to March 31, 2026, to provide reasonable assurance that LTG'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 LTG's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period April 1, 2025 to March 31, 2026, to provide reasonable assurance that LTG'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 LTG's controls operated effectively throughout that period.

Art Machado

Art Machado
Vice President of Information Security
Learning Technologies Acquisition Corporation

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Learning Technologies Acquisition Corporation

Scope

We have examined LTG's accompanying description of its SaaS Offering Services System titled "Learning Technologies Acquisition Corporation's Description of Its SaaS Offering Services System throughout the period April 1, 2025 to March 31, 2026" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2025 to March 31, 2026, to provide reasonable assurance that LTG's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

LTG uses AWS to provide cloud hosting services, Centersquare and Digital Realty to provide data center hosting and customer storage services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at LTG, to achieve LTG's service commitments and system requirements based on the applicable trust services criteria. The description presents LTG's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of LTG'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 LTG, to achieve LTG's service commitments and system requirements based on the applicable trust services criteria. The description presents LTG's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of LTG's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

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

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

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

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

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

Independence and Ethical Responsibilities

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

Inherent Limitations

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

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

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

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects,

a. the description presents LTG's SaaS Offering Services System that was designed and implemented throughout the period April 1, 2025 to March 31, 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period April 1, 2025 to March 31, 2026, to provide reasonable assurance that LTG'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 LTG's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period April 1, 2025 to March 31, 2026, to provide reasonable assurance that LTG'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 LTG'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 LTG, user entities of LTG's SaaS Offering Services System during some or all of the period April 1, 2025 to March 31, 2026, business partners of LTG subject to risks arising from interactions with the SaaS Offering 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
May 7, 2026

SECTION 3

LEARNING TECHNOLOGIES ACQUISITION CORPORATION'S DESCRIPTION OF ITS SAAS OFFERING SERVICES SYSTEM THROUGHOUT THE PERIOD APRIL 1, 2025 TO MARCH 31, 2026

OVERVIEW OF OPERATIONS

Company Background

Learning Technologies Acquisition Corporation (‘LTG’ or ‘the Company’) provides integrated talent management, learning, and workforce compliance Software-as-a-Service solutions.

Description of Services Provided

The Company’s solutions are delivered in a SaaS model, collectively referred to as the SaaS Offerings, and include the following commercial applications:

- Affirmity
- Breezy HR
- Bridge Talent Suite (also Bridge Skills Plus, Bridge Learn & Develop)
- Bridge Perform
- Bridge Engage
- Bridge Full Suite
- Gomo (also Bridge Advanced Authoring)
- Instilled (also Bridge Advanced Video, Bridge Advanced Media)
- Open LMS
- PeopleFluent Communications
- PeopleFluent Learning (NetDimensions)
- PeopleFluent OrgPublisher
- PeopleFluent Recruiting
- PeopleFluent Talent Acquisition ('RMS')
- PeopleFluent Compensation
- PeopleFluent Talent Performance
- PeopleFluent Talent Succession
- PeopleFluent Talent Management
- PeopleFluent Talent Management - Recruiting
- Reflektive
- Rustici Content Controller, Managed Hosting
- Rustici Engine, Managed Hosting
- Rustici Software SCORM Cloud
- Watershed LRS

The descriptions provided in the remainder of this section do not encompass every aspect of the SaaS Offerings provided or procedures followed within the Company. Rather, the descriptions enable current and future user entities to understand how controls in place for the SaaS Offerings are critical to the Company’s business and overall control environment.

Principal Service Commitments and System Requirements

The Company designs its processes, policies, and procedures related to the SaaS Offerings to meet Company objectives. These objectives are based on the service commitments that the Company makes to customers, the laws and regulations applicable to the SaaS Offerings, and the financial, operational, and compliance requirements that the Company has established.

Security, Availability, and Confidentiality commitments to customers are documented and communicated to customers in the Service Level Agreement ('SLA') and Terms and Conditions. These commitments include, but are not limited, to the following:

Trust Service Category	Service Commitments	System Requirements
Security	• Limit system access to authorized personnel only • Protect data in transit and at rest • Develop secure code • Segment networks according to function • Enforce strong passwords and two-factor authentication for privileged access • Perform regular security assessments • Identify and remediate security events and incidents • Develop, enforce and maintain an information security program to protect the Service	• Logical access standards • Access provisioning and deprovisioning standards • Quarterly access reviews • Encryption standards • Security monitoring and alerting • Vulnerability management standards • Risk management standards • Security event response plan • Change management standards
Availability	• Provide service uptime to meet committed SLAs • Maintain recovery capability for systems and data • Respond to availability issues in accordance with SLAs	• Backup and restoration capabilities • System monitoring • Communication channels for reporting issues
Confidentiality	• Keep customer data confidential and prevent unauthorized disclosure • Notify promptly in the event of a security breach or unauthorized disclosure of confidential information	• Information classification • Data retention and destruction standards • Confidentiality standards • Breach notification standards

Components of the System

Infrastructure

The primary types of infrastructure components used to deliver the Company's SaaS Offering Services System are the following:

- Firewalls
- Routers
- Storage Area Network ('SAN') Storage
- Switches
- Virtualization Servers

Software

The primary types of software components used to deliver the Company's SaaS Offering Services System are the following:

- Antivirus and Malware/Zero-day Protection
- Application Infrastructure (inclusive of Web Services, Databases, Application Engines, Shared Application Programming Interface Services, and Integration Middleware)
- Data Leak Prevention
- Firewalls
- Intrusion Detection and Prevention
- Log management
- Monitoring
- Operating Systems
- Web Application Load Balancers

People

Oversight of the control framework that supports The Company's organizational environment starts with its Executive Team and is supported by Department Managers and other team members in the following functional areas:

- Executive Team - led by the Managing Directors of the Company's business units providing the SaaS Offerings, provides direction and oversight of the supporting functions
- Information Security - led by the Vice President ('VP') of Information Security, provides strategic and operational oversight of the Company's security, privacy, compliance, and vendor risk assessment responsibilities
- System Administration - led by the VP of Hosting Systems and Operations (or business unit-specific equivalent), responsible for effective provisioning, installation/configuration, operation, and maintenance of systems and environments related to the Company's SaaS Offerings
- Customer Support - led by the VP of Customer Support (or business unit-specific equivalent), provides first level support for client issues as well as escalating more severe problems to appropriate departments
- Client Services - led by the VP of Professional Services (or business unit-specific equivalent), provides project management and client implementation services related to the Company's SaaS Offerings
- Engineering - led by the VP of Software Engineering (or business unit-specific equivalent), performs product management, development, and quality assurance for planning, building, and maintaining the Company's SaaS applications
- Human Resources - led by the Chief People Officer, provides support services for the personnel that deliver and manage the Company's SaaS Offerings. This includes onboarding/off-boarding of employees, security and compliance training, and the employee performance review process

Data

The Company may collect personal data from customers as allowed for in its Service Agreements and to the extent necessary for provisioning the SaaS Offerings. Customers also routinely submit customer data to the Company in the course of utilizing the SaaS Offerings. Hosted data includes any data created, uploaded or transmitted as part of the functioning of the SaaS Offerings, as determined by the customer.

The Company has a Data Classification Policy that outlines the various types of data created, collected, processed and stored by the Company's SaaS Offerings. This policy identifies different levels of confidentiality and the respective care required when handling such data. The Company has also codified Data Retention and Destruction Policies to govern how data is stored and deleted. Data management processes are aligned with this policy, ensuring that the Company retains and destroys data appropriately. The Company uses secure protocols for customers to enter, upload, or otherwise transmit customer data.

Processes, Policies and Procedures

The Company has developed and communicated to its personnel policies and procedures to protect customer information and Company assets. Policies and procedures are documented and updated on the Company intranet to ensure personnel are informed and equipped to perform their duties to preserve security, availability of the SaaS Offerings, and confidentiality of customer data. These documents include but are not limited to the following areas:

- Acceptable Use Policy
- Access Management Policy
- AI Policy
- Asset Management Policy
- Bring Your Own Device Policy
- Business Continuity Planning and Disaster Recovery Policy
- Change Management Policy and Procedures
- Client Data Privacy Compliance Policy
- Customer Onboarding/Offboarding Procedures
- Data Backup Policy
- Data Classification and Handling Policy
- Data Encryption Policy
- Data Privacy Compliance Policy
- Data Retention, Destruction and Disposal Policy
- Encryption Key Management Policy
- End-of-Life Software Policy
- Global Information Security Training for Contractors Policy
- Information Security Statement
- Internal Audit and Compliance Policy
- Password Policy
- Patch Management Procedures
- Physical Security Policy
- Risk Management Policy
- Secure Software Development (SDLC) Policy
- Security Baselines Policy
- Security Incident Response Plan
- Vendor Management Policy
- Vulnerability Management Policy

Physical Security

The SaaS Offerings are hosted by multiple data center providers. As such, the physical access responsibilities are carved-out to the Subservice Organizations. Please refer to the 'Subservice Organizations' section below.

Logical Access

The Company implements role-based, named user access controls to Company application systems. New hires are granted access according to their job roles, only receiving access to what is required to carry out their responsibilities. The Human Resources ('HR') team works with hiring managers to specify these job roles. The least privilege principle is rigorously applied.

Privileged access, such as access to the production environment, requires explicit approval. Employees and contractors submit requests for administrative access to the production environment which are reviewed and approved by Hosting management. Production access is only provisioned once the request has been approved. The quality assurance ('QA') and development environments are kept logically separate from the production environment to further protect the production environment.

Upon termination, employee and contractor access to the production environment is promptly revoked. Terminations are communicated to Information Technology ('IT') personnel in advance whenever possible to allow sufficient time for processing access removals. The use of a Single Sign-On ('SSO') system helps minimize the work required to properly handle employee access during offboarding.

On top of tight controls around provisioning and deprovisioning access, the Company has built in redundancy of its controls by performing quarterly user access reviews. System owners audit the lists of users with access to production environments and production critical systems to ensure access is appropriate. Any deficiencies found are promptly remediated.

In accordance with its Access Management policies, the Company enforces secure practices for employee access to systems, including the use of Multi-Factor Authentication ('MFA'), strong passwords and network policies. Access to production environments are configured to strictly enforce MFA. Password best practices are enforced through system configurations. Critical access is only possible through the Hosting network, which is isolated from the corporate and guest networks to limit the Company's attack surface.

Vulnerability and Incident Management

Proactive incident prevention methods are in place to reduce the likelihood of incidents. IT personnel use mobile device management tools to enforce antivirus software and full disk encryption for workstations, firewall configurations, data loss prevention, and remote wipe policies. Delinquent devices are surfaced to IT personnel to remediate and ensure endpoint protection is updated and operating properly.

The Company uses specialized tools to perform dynamic and static application security scanning of its applications, as well as software composition analysis to identify vulnerabilities in third-party code. These scans are automated to run regularly and report both the number and severity of identified vulnerabilities. Having awareness of these vulnerabilities allows the Company's personnel to effectively target their efforts, prioritizing the most critical issues to ensure the SaaS Offerings remain secure and operational. At least annually, the Company also engages a specialized third-party testing firm to perform penetration tests against the SaaS Offerings. Validated findings are remediated in a timely manner that aligns with the Company's internal vulnerability remediation SLA.

In addition, the Company has implemented intrusion detection and prevention capabilities that are integrated with the SaaS Offerings to proactively detect and prevent security events with a high degree of accuracy. In most cases, suspicious activity is prevented before there is impact to the SaaS Offerings requiring minimal action by the Hosting team. Nonetheless, the Hosting team maintains high visibility of security events through monitoring systems which provide 24/7 alerting to an on-call security team. In the rare occasions where further action is required, the Hosting team investigates and takes actions to resolve security events that continue to pose a threat. In the event that threats circumvent the above measures, the Company encourages customers and employees to report issues or security incidents. By working with both internal and external parties, the Company expands its security framework and increases visibility into potential threats through a layered-defense approach. Prompt identification is crucial to minimizing the impact of an incident.

While many measures are implemented to prevent or minimize the occurrence and impact of incidents, the Company recognizes the importance of preparing for such scenarios. Thus, the Company has developed a Security Event Response Plan ('SERP') that guides personnel in response and resolution. Events that may impact security, availability or confidentiality are identified, tracked, and escalated as appropriate. Appropriate personnel are assigned to investigate and respond. Detailed records of these events are maintained to aid in tracking resolution and for future reference. These procedures keep the Company's personnel equipped to contain, resolve and recover from identified incidents. The company conducts annual tabletop exercises to ensure personnel are prepared and well versed in the SERP, simulating various incidents and rehearsing response activities. These dry runs offer an opportunity to identify areas of improvement to continually adapt the SERP to the changing threat landscape. Once an incident has been resolved, the Company performs a post-mortem to better understand the root cause and progression of the incident. This analysis yields valuable insights to prevent future incidents. Upon assessing the consequences of the incident, the Company determines whether customer notification is required. Customers are contacted as needed to communicate potential impacts and recommended actions. Once an incident has been resolved, the Company performs a post-mortem to better understand the root cause and progression of the incident. This analysis yields valuable insights to prevent future incidents.

The company conducts annual tabletop exercises to ensure personnel are prepared and well versed in the Security Event Response Plan (SERP), simulating various incidents and rehearsing response activities. These dry runs offer an opportunity to identify areas of improvement to continually adapt the SERP to the changing threat landscape.

In rare instances, an incident may be so severe that it is classified as a disaster. The Company has established Disaster Recovery Plans to direct personnel on how to handle such circumstances. The plans prioritize bringing the SaaS Offerings back to a secure and stable state as soon as possible while minimizing impact to the Company and its customers. The Company conducts annual tests to validate the efficacy of the Disaster Recovery Plans and ensure established plans can be reliably carried out. Identified shortcomings are addressed to improve recovery capabilities. Disaster recovery tests and notable updates to the Disaster Recovery Plans are documented for future reference.

Change Management

The Company has formulated change management policies and procedures that guide personnel on best practices to ensure the SaaS Offerings are developed and maintained properly. These documents are regularly reviewed and updated by the Hosting team. The documented change process requires that changes be approved before implementation to prevent unauthorized modifications that may impact the SaaS Offerings or customers. Each change request is documented, requiring review and approval. Once approved, the change is monitored through successful implementation. Change documentation is updated when the change has been successfully completed or abandoned, and post-mortem analysis is performed as needed to drive continuous improvement.

System Operations

The Company takes steps to ensure data transmission between customers and the Company's servers are protected. Secure protocols and encryption are utilized to keep customer data secure. These measures reduce the risk of data loss or exposure during transit to the Company's custody.

The Company utilizes monitoring tools to provide visibility into the SaaS Offerings' performance and availability. These tools are configured to alert the Hosting team based on predefined thresholds. Upon receipt of an alert, Hosting personnel review and triage the issue for investigation and resolution.

System operations are further supported through capacity and configuration management functions. The production environment takes advantage of auto-scaling functionality to scale resource capacity within defined thresholds to meet demand as needed. Auto-scaling ensures customers can enjoy high availability of the SaaS Offerings even during peak times without the need for manual capacity management. Configuration management capabilities are leveraged to detect configuration drift and restore variances back to approved baseline configurations. This reduces the risk of misconfigurations disrupting the production environment and causing issues for customers.

The Company ensures high reliability and stable uptime of the SaaS Offerings by implementing measures to protect against data loss. Geographically distributed database redundancy and failover capabilities provide customers confidence that their data can be reliably accessed even in the event of a local disaster.

The Company also performs daily backups and implements backup archival strategies that ensure backups are maintained for up to a year. Refer to the ‘Subservice Organizations” section below for additional details. These backups are encrypted at rest and tested at least annually to ensure that the Company can reliably restore from any given backup. Employees are equipped with well documented backup and restoration procedures to reference during these tests and if required, address an incident. Backup retention procedures are in place to enforce the specifications laid out in the Data Retention, Destruction and Disposal Policy.

Boundaries of the System

The scope of this report includes the SaaS Offering Services System delivered by the Company headquartered in Raleigh, North Carolina and supporting controls performed remotely by the Company's personnel.

This report does not include the subservice organizations, such as AWS for cloud hosting services and Centersquare and Digital Realty for its data center hosting and customer storage services.

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

Control Environment

Customer Commitments and Communication

The Company communicates details about the SaaS Offerings and the Company’s commitments to Security, Availability, and Confidentiality in the SLA and Standard Terms and Conditions (collectively, the Terms) of its Service Agreements with customers. The SLA sets customer expectations of the quality of the SaaS Offerings while the Terms sets customer expectations on the types of controls The Company has implemented. Customers acknowledge understanding of the Company’s commitments upon signing a Master Service and License Agreement (‘MSLA’).

The Company strives to provide resourceful information to customers. The Company’s support websites provide access to comprehensive product documentation, as well as information on troubleshooting and best practices, and guidance on how to report problems and seek additional support. As the Company continues to improve its SaaS Offerings, new releases may impact various aspects of the customer experience. The Company posts release notes that are available to relevant customers and that describe recent product changes, potential impacts to customers and any changes that affect security, availability, or confidentiality commitments.

Measures are in place to protect customer data entrusted to the Company's custody. Databases are configured to segregate each customer's data and limited to designated global regions for compliance purposes where applicable. Customer data segregation protects the confidentiality of customer data by preventing one customer from accessing the data of another customer. If there is a need to replicate or use sensitive customer data outside of the production environment, the Company requires prior written authorization from the customer, and agreement on any applicable anonymization or sanitization requirements.

Customers are off boarded upon termination of their service periods. The company retains and destroys customer data in accordance with its Data Retention and Data Destruction Policies, and any overriding contractual commitments to specific customers. Customers may request that their data be purged by contacting the Company.

HR Policies and Practices

The Company believes that hiring qualified individuals is essential to achieving Company objectives. The Company has established robust hiring practices that begin with a cooperative effort between HR and hiring managers to develop job descriptions that specify candidate requirements, expectations, and responsibilities of the role. Qualified candidates undergo a rigorous background check to confirm that the new hires meet Company standards. Background checks should be completed before access to applications that impact the production environment or contain customer data is granted. Upon hire, employees are required to read, understand and formally acknowledge the Company's policies and confidentiality requirements. Employees specifically acknowledge their commitment to confidentiality by signing a confidentiality agreement.

The Company continues to support employee success after the initial hiring process. Employees are made aware of reporting lines and key roles in the Company to ensure personnel are knowledgeable of available resources both within and outside of their particular reporting line. The Company's Human Resources Information System ('HRIS') automatically updates and maintains an organizational chart to provide employees a reference for the organizational structure.

New employees undergo Security Awareness Training ('SAT') to ensure personnel follow best security practices. This training is refreshed annually with a Company-wide SAT that addresses common threats in the current threat landscape, as well as information about important security and privacy procedures and obligations.

The Company understands the significant value of input from its personnel. Formal performance reviews with employees and their managers occur at least annually via performance management tools. These reviews provide employees with feedback on their performance and offer an opportunity for employees to voice their individual goals, motivations and company goals. Managers can utilize this time to better understand their team members and identify training or developmental opportunities that may further develop their skills and reach company objectives.

Aside from frequent check-ins, employees are also encouraged to report misconduct and grievances through an independent third-party whistle-blower channel to further foster a productive, ethical and safe work environment. Submissions are kept confidential and investigated thoroughly by designated representatives. If fraud or other misconduct is identified as a result of investigation, findings are reported to the Board for resolution.

Organizational Management

The control environment reflects the Company philosophy emphasizing the importance of integrity and ethical values. The Company sets this tone from the top and leads by example. The Board and Executive Management agree to Standards of Conduct that establish the basis for acceptable behavior. The Standards of Conduct are communicated to personnel, and Management ensures that employees remain committed to these values by enforcing sanctions on employees found to be delinquent. These sanctions include written warnings, suspension and termination as possible consequences of misconduct or failure to comply with Company policies.

The Company's management also regularly communicates with personnel regarding organizational strategies and objectives, and how employee roles and responsibilities support these strategies and objectives.

Internal Communication

Efficient and effective operation of a control environment requires strong internal communication practices. Communication begins with making sure relevant information is widely available and accessible for employees. General security practices and Company expectations are outlined in the Company's Information Security Policies, which are available to employees on the Company intranet. Employees can refer to this documentation for guidance on day-to-day requirements and best practices. The Information Security Policies are maintained and updated annually by the Security team for consistency with the ever-changing technology and security landscape and to align with operational changes as the Company continues to mature.

The Information Security Policies inform employees how to properly handle customer data in the Company's custody and to protect its security, confidentiality, and availability at all times. Additionally, the Company has codified various levels of data sensitivity, so employees know how to treat the data with appropriate caution. The Data Classification Policy offers numerous examples of each data classification to minimize ambiguity.

The Company also maintains extensive additional policy and procedural documentation covering the broader functions involved in configuring and running its production systems, and the procedural specifics of implementing its Information Security Policies.

Risk Management

The Company conducts a comprehensive annual risk assessment to stay proactive in mitigating risks. The risk assessment process is overseen by the Executive Security Steering Committee, which is composed of executive management from various departments. The risk assessment identifies security risks as well as fraud and vendor risks to the SaaS Offerings, organization and data. Risks are scored by likelihood and impact to determine criticality. Risks that exceed the Company's risk tolerance are prioritized and treated accordingly. Risk treatment options include risk modification, risk avoidance, risk sharing and risk retention. Remediation actions are tracked continually throughout the year to ensure risk treatment efforts are completed and effective. The procedure for conducting a risk assessment is summarized as follows:

- Establish Context. The Company first establishes context for the risk assessment by defining the risk acceptance criteria against which the risk analysis will be compared and evaluated. Risk acceptance criteria depend on context, such as Company policies, goals, objectives, stakeholder interests, laws, and regulations
- Identify Risks. Once the context and risk criteria have been established, a controls-based approach is used to identify the risks of not having certain controls in place. These may be from an absence of a control, or a weakness in an existing control identified as exceptions during an audit. These risks are identified internally within the Company as well as externally for vendors. The Company reviews vendor security reports to identify external risks from vendors
- Analyze Risks. The level of risk is calculated by estimating the likelihood of a threat and its impact on the business

- Evaluate Risks. Risks are evaluated by comparing the risk analysis results with the risk acceptance criteria. The context that was established at the beginning of the risk assessment process guides management in determining whether or not the risks are acceptable
- Risk Treatment. Risk treatment is determined for each identified risk. There are four risk treatment options: 1) risk modification, 2) risk avoidance, 3) risk sharing, and 4) risk retention:
    - Risk modification involves selecting and implementing controls to mitigate risk to an acceptable level
    - Risk avoidance involves withdrawing or discontinuing an activity that is vulnerable to risk. The negative costs of a certain activity may be deemed to outweigh its benefits
    - Risk sharing involves another party sharing the burden of loss or benefit of gain for a risk. For example, The Company can pay an insurance company to share the responsibility of damage from a threat event. The business impact of such an event and, therefore, the level of risk is reduced
    - Risk retention is the acceptance of the burden of loss or benefit of gain from a particular risk. Certain risks may be accepted based on risk evaluation. However, some risks, such as those that could result in non-compliance with laws and regulations, may not be accepted
- Communication and Monitoring. The Company produces a risk treatment plan that outlines how risk treatment will be implemented at the Company. This plan is communicated to management for approval and to relevant departments for execution. The risk assessment and risk treatment process are documented and reviewed to continually improve the Company's risk management after each iteration

The risk assessment process includes an evaluation of existing controls in place at the Company. For instance, a risk may be scored high if an existing control is ineffective in mitigating the risk. Management utilizes this information to determine whether to replace the control or redesign the control. In the event that a gap in the control environment is identified, management assesses what controls are needed for the coverage of a risk. Findings from the risk assessment are included in at least annual control reviews conducted to monitor the progress of remediation.

Vendor Management

The Company has formulated a vendor management program that oversees vendor relationships and assesses impacts to Company commitments and objectives. New vendors undergo a thorough review prior to onboarding that includes assessment of contracts, certifications and compliance reports. This process enables the Company to identify whether the vendor's controls reflect commensurate coverage and commitment to the Company's security standards and commitments to its customers. The Company performs an annual review, reassessing the ongoing vendor relationships to confirm that vendors can continue to meet its high standards of Security, Availability, and Confidentiality.

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, Availability, and Confidentiality criteria were applicable to the SaaS Offering Services System.

Subservice Organizations

This report does not include the subservice organizations, such as AWS for cloud hosting services and Centersquare and Digital Realty for its data center hosting and customer storage services.

At least annually, the Company obtains and reviews the Subservice Organization SOC 2 examination reports. As part of the review process, the Company assesses the adequacy of controls in place at the Subservice organizations to ensure that the combination of measures implemented by the Company and the Subservice Organizations sufficiently addresses the Company's business, legal, security and compliance commitments.

Subservice Description of Services

AWS

The Company uses AWS infrastructure for cloud hosting and storage for customers. Physical data center backups were transitioned to AWS storage in February 2025. AWS provides robust security capabilities for organizations to implement and maintain security and data protection. AWS has achieved many compliance certifications to provide customers assurance that its platform meets customer security requirements and industry standards. Such compliance certifications and assurance programs include Payment Card Industry ('PCI') Data Security Standards ('DSS') Level 1, Service Organization Controls ('SOC') 1, SOC 2, SOC 3, FedRAMP, International Organization for Standardization ('ISO') 27001, Multi-Tier Cloud Security Level 3 certification, and Cloud Security Alliance certification.

Centersquare

The Company uses Centersquare for its physical infrastructure services used to provide hosting and storage for customers. Centersquare provides robust security capabilities for organizations that host their own hardware and maintain physical plant security, power, and cooling diversity for the systems. Centersquare undergoes rigorous third-party assurance processes, including SSAE 18/ ISAE 3402 SOC 1 Type 2, SSAE 18/ ISAE 3000 SOC 2 Type 2, ISO 27001, PCI DSS 3.2.1, to ensure that it is meeting customer security requirements and industry standards.

Digital Realty

The Company uses Digital Realty for its physical infrastructure services used to provide hosting and storage for customers. Digital Realty provides robust security capabilities for organizations that host their own hardware and maintain physical plant security, power, and cooling diversity for the systems. Digital Realty undergoes rigorous third-party assurance processes, including SSAE 18/ ISAE 3000 SOC 2 Type 2, ISO 27001, PCI DSS 3.2.1, to ensure that it is meeting customer security requirements and industry standards.

Complementary Subservice Organization Controls

The Company uses Subservice Organizations, AWS for cloud hosting services, Centersquare for data center hosting and customer storage services, and Digital Reality for its data center hosting and customer storage services. In the design of the SaaS Offerings' controls, management expects the following types of controls to be suitably designed and operating effectively at the Subservice Organizations to meet certain applicable Trust Services Criteria. Such controls are referred to as complementary subservice organization controls ('CSOCs'):

Criteria	Type of Controls Expected at the Subservice Organizations
CC6.1	• Logical controls are in place to prevent unauthorized access to the production infrastructure and customer data • Customers are restricted from accessing the underlying backend infrastructure or the data of other customers • Encryption keys are managed and stored in accordance with defined policies and procedures • Customer data is encrypted at rest
CC6.3	• Access to data and software is restricted to personnel authorized and provisioned with logical security controls
CC6.4	• Physical access to the data center facility is restricted to data center personnel
CC6.5	• Procedures for securely decommissioning storage devices that have reached the end of their useful life are established to prevent customer data from being exposed to unauthorized individuals
CC6.6	• Security groups are configured to restrict access to the production environment. Changes to security groups are restricted to authorized personnel
CC6.7	• Encryption is used to protect customer data in transit between the customer and the Subservice Organization
CC6.8	• Entity implements controls to prevent or detect, and act upon unauthorized or malicious software to meet the entity's objectives
CC7.1	• Changes to application, infrastructure and configurations require review and approval from management • Vulnerability tests are conducted. Identified vulnerabilities are reviewed and remediated in accordance with their criticality
CC7.2	• Logging and monitoring are in place to detect anomalies indicative of malicious activity
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
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
CC7.5	• The entity identifies, develops, and implements activities to recover from identified security incidents
CC9.1	• The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions

Criteria	Type of Controls Expected at the Subservice Organizations
CC9.2	• The entity assesses and manages risks associated with vendors and business partners
A1.1	• System capacity is monitored on an ongoing basis for Subservice organization services. Capacity is added when defined thresholds are exceeded, or as needed
A1.2	• Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, approved, maintained, and monitored to meet the Subservice Organization's availability commitments • Backups are monitored for success and failure. Failures are investigated and resolved in a timely manner
A1.3	• Disaster recovery capabilities are reviewed and tested annually against recovery objective service commitments

The Company's management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet the relevant Trust Services Criteria through written contracts, such as service level agreements. In addition, The Company performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding discussions with vendors and subservice organizations at least annually
- Reviewing attestation reports over services provided by vendors and subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

The SaaS Offerings were designed with the assumption that certain controls would be implemented by the user entity. In certain situations, the application of specific controls at user organizations is necessary to achieve certain control objectives included in this report.

This section describes additional controls that should be in operation at the user entity to complement the controls at the Company. However, there may be control objectives or related controls not identified in this report, which may be appropriate for a specific user entity. The CUECs listed below should not be considered a complete or comprehensive list that should be employed by a user entity. User entities should consider whether the following controls have been placed in operation at their organizations:

Criteria	Complementary User Entity Controls
CC2.1	• Controls over reviewing the completeness and accuracy of the reports that are produced by the SaaS Offerings
CC2.3	• Controls to report any material changes to the user entity's overall control environment, in a timely manner, that may adversely affect the SaaS Offerings
CC6.1	• Controls over the use of Identification Documents ('IDs') and passwords that are used to access the SaaS Offerings • Controls to provide reasonable assurance that the user organization's method for accessing the SaaS Offerings is configured with proper logical security controls • Controls to provide reasonable assurance that only authorized individuals from the user entity are granted the ability to access, modify, and delete information from the SaaS Offerings • Controls to request deletion of user entity's data, if applicable

Criteria	Complementary User Entity Controls
CC6.3	• Controls to provide a reasonable assurance that user accounts and access permissions are correctly specified on an ongoing basis, including revoking accounts
CC6.7	• Controls to protect transmitted data using appropriate methods to ensure confidentiality, integrity, availability, and non-repudiation
CC6.8	• Controls to provide reasonable assurance that changes to processing options (parameters) are appropriately authorized, approved, and implemented • Controls to implement controls requiring additional approval procedures for critical transactions relating to the SaaS Offerings

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security, Availability, and Confidentiality Categories)

Security refers to the protection of:

i. information during its collection or creation, use, processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability

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

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Control 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 The Company's description of the system. Any applicable Trust Services Criteria that are not addressed by control activities at The Company are described within Section 4 and within the Subservice Organization 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 LTG was limited to the Trust Services Criteria, related criteria and control activities specified by the management of LTG and did not encompass all aspects of LTG'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.	Personnel are provided access to and required to review relevant company policies, code of conduct, and statement of confidentiality upon hire.	Inspected the company's intranet, the new hire onboarding e-mail, the onboarding and confidentiality acknowledgment for a sample of new hires, and the code of conduct acknowledgment for a sample of new hires to determine that personnel were provided access to and required to review relevant company policies, code of conduct, and statement of confidentiality upon hire.	No exceptions noted.
		Management has developed a background check policy to ensure individuals are being hired based on an acceptable background and skills requirements for the given position.	Inspected the global background check policy to determine that management has developed a background check policy to ensure individuals were being hired based on an acceptable background and skills requirements for the given position.	No exceptions noted.
		Personnel are required to undergo a background check upon hire, where permissible by applicable laws.	Inspected the completed background check for a sample of new hires to determine that personnel were required to undergo a background check upon hire, where permissible by applicable laws.	No exceptions noted.
		Performance reviews are performed at least annually.	Inquired of the Vice President of Information Security regarding the performance evaluation process to determine that performance reviews were performed at least 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 review policy to determine that performance reviews were performed at least annually.	No exceptions noted.
			Inspected the performance evaluation form for a sample of current employees to determine that performance reviews were performed at least annually.	Testing of the control activity disclosed that a performance review was not performed on an annual basis for two of 40 current employees sampled.
		Management monitors compliance with training requirements.	Inspected the training completion summary report to determine that management monitored compliance with training requirements.	No exceptions noted.
		Core values are documented and communicated via company intranet from executive management to personnel.	Inquired of the Vice President of Information Security regarding the company's intranet to determine that core values were documented and communicated via company intranet from executive management to personnel.	No exceptions noted.
			Observed the company's intranet to determine that core values were documented and communicated via company intranet from executive management to personnel.	No exceptions noted.
			Inspected the company's business newsletter and company's intranet to determine that core values were documented and communicated via company intranet from executive management to personnel.	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**
		Management has established a policy and procedure for reporting, handling, and resolving complaints including violations of the code of conduct.	Inspected the code of conduct policy to determine that management has established a policy and procedure for reporting, handling, and resolving complaints including violations of the code of conduct.	No exceptions noted.
		A reporting mechanism is in place to allow employees to report unethical behavior in a confidential manner.	Inspected the whistleblowing policy to determine that a reporting mechanism was in place to allow employees to report unethical behavior in a confidential 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.	Management meets with Board Members and/or committees at least annually to provide information about Company's control effectiveness.	Inquired of the Vice President of Information Security regarding the annual report to determine that management met with Board Members and/or committees at least annually to provide information about Company's control effectiveness.	No exceptions noted.
			Inspected the information security statement, the security document overview, and the annual report to determine that management met with Board Members and/or committees at least annually to provide information about Company's control effectiveness.	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**
		Executive management meets at least annually with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected the completed security and privacy objectives, the Executive Security Steering Committee meeting minutes and slide deck to determine that executive management met at least annually with operational management to assess the effectiveness and performance of internal controls within the environment.	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.	Performance reviews are performed at least annually.	Inquired of the Vice President of Information Security regarding the performance evaluation process to determine that performance reviews were performed at least annually.	No exceptions noted.
			Inspected the performance review policy to determine that performance reviews were performed at least annually.	No exceptions noted.
			Inspected the performance evaluation form for a sample of current employees to determine that performance reviews were performed at least annually.	Testing of the control activity disclosed that a performance review was not performed on an annual basis for two of 40 current employees sampled.
		An organizational chart is in place to communicate to personnel assigned responsibilities and lines of authority within management.	Inspected the organizational chart to determine that an organizational chart was in place to communicate to personnel assigned responsibilities and lines of authority within 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**
		Employee goals and objectives are used to frame performance evaluations.	Inquired of the Vice President of Information Security regarding the performance evaluation process to determine that employee goals and objectives were used to frame performance evaluations.	No exceptions noted.
			Inspected the employee performance review policy and the employee hub and manager review preparation sheet to determine that employee goals and objectives were used to frame performance evaluations.	No exceptions noted.
		Executive management meets at least annually with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected the completed security and privacy objectives, the Executive Security Steering Committee meeting minutes and slide deck to determine that executive management met at least annually with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.
		The entity qualifies and performs initial and thereafter annual risk assessments for its vendors.	Inquired of the Governance, Risk and Compliance Analyst regarding vendor management to determine that the entity qualified and performed initial and thereafter annual risk assessments for its 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 management policy, the completed vendor risk assessment, and the completed vendor risk assessment for a sample of new and existing vendors to determine that the entity qualified and performed initial and thereafter annual risk assessments for its 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.	Personnel are required to undergo a background check upon hire, where permissible by applicable laws.	Inspected the completed background check for a sample of new hires to determine that personnel were required to undergo a background check upon hire, where permissible by applicable laws.	No exceptions noted.
		Performance reviews are performed at least annually.	Inquired of the Vice President of Information Security regarding the performance evaluation process to determine that performance reviews were performed at least annually.	No exceptions noted.
			Inspected the performance review policy to determine that performance reviews were performed at least annually.	No exceptions noted.
			Inspected the performance evaluation form for a sample of current employees to determine that performance reviews were performed at least annually.	Testing of the control activity disclosed that a performance review was not performed on an annual basis for two of 40 current employees sampled.

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**
		Management monitors compliance with training requirements.	Inspected the training completion summary report to determine that management monitored compliance with training requirements.	No exceptions noted.
		Employee goals and objectives are used to frame performance evaluations.	Inquired of the Vice President of Information Security regarding the performance evaluation process to determine that employee goals and objectives were used to frame performance evaluations.	No exceptions noted.
			Inspected the employee performance review policy and the employee hub and manager review preparation sheet to determine that employee goals and objectives were used to frame performance evaluations.	No exceptions noted.
		Continued training is required annually for technical employees to ensure applicable skills remain current.	Inquired of the Vice President of Information Security regarding the secure development training to determine that continued training was required annually for technical employees to ensure applicable skills remain current.	No exceptions noted.
			Inspected the information security statement, the secure development training tracker, and the completed continued technical training for a sample of technical employees to determine that continued training was required annually for technical employees to ensure applicable skills remain current.	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 take an annual information security training.	Inquired of the Vice President of Information Security regarding the information security training to determine that personnel were required to take an annual information security training.	No exceptions noted.
			Inspected the information security training materials, the information security statement, and the completed information security training for a sample of current employees to determine that personnel were required to take an annual information security training.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Personnel are provided access to and required to review relevant company policies, code of conduct, and statement of confidentiality upon hire.	Inspected the company's intranet, the new hire onboarding e-mail, the onboarding and confidentiality acknowledgment for a sample of new hires, and the code of conduct acknowledgment for a sample of new hires to determine that personnel were provided access to and required to review relevant company policies, code of conduct, and statement of confidentiality upon hire.	No exceptions noted.
		Performance reviews are performed at least annually.	Inquired of the Vice President of Information Security regarding the performance evaluation process to determine that performance reviews were performed at least 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 review policy to determine that performance reviews were performed at least annually.	No exceptions noted.
			Inspected the performance evaluation form for a sample of current employees to determine that performance reviews were performed at least annually.	Testing of the control activity disclosed that a performance review was not performed on an annual basis for two of 40 current employees sampled.
		An organizational chart is in place to communicate to personnel assigned responsibilities and lines of authority within management.	Inspected the organizational chart to determine that an organizational chart was in place to communicate to personnel assigned responsibilities and lines of authority within management.	No exceptions noted.
		Employee goals and objectives are used to frame performance evaluations.	Inquired of the Vice President of Information Security regarding the performance evaluation process to determine that employee goals and objectives were used to frame performance evaluations.	No exceptions noted.
			Inspected the employee performance review policy and the employee hub and manager review preparation sheet to determine that employee goals and objectives were used to frame performance evaluations.	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**
		Executive management meets at least annually with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected the completed security and privacy objectives, the Executive Security Steering Committee meeting minutes and slide deck to determine that executive management met at least annually with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.
		The entity qualifies and performs initial and thereafter annual risk assessments for its vendors.	Inquired of the Governance, Risk and Compliance Analyst regarding vendor management to determine that the entity qualified and performed initial and thereafter annual risk assessments for its vendors.	No exceptions noted.
			Inspected the vendor management policy, the completed vendor risk assessment, and the completed vendor risk assessment for a sample of new and existing vendors to determine that the entity qualified and performed initial and thereafter annual risk assessments for its vendors.	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**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Hosted products are designed to support multiple levels of access.	Inspected the levels of access to determine that hosted products were designed to support multiple levels of access.	No exceptions noted.
		Policies and procedures are documented for significant processes and are available on the entity's intranet.	Inspected the security documentation overview and the entity's intranet to determine that policies and procedures were documented for significant processes and were available on the entity's intranet.	No exceptions noted.
		The Company reviews the control environment during the annual risk assessment to determine whether its controls need to be added, modified, or removed.	Inspected the completed risk assessment, the completed security and privacy objectives, and the Executive Security Steering Committee meeting minutes to determine that the Company reviewed the control environment during the annual risk assessment to determine whether its controls need to be added, modified, or removed.	No exceptions noted.
		The VP of Information Security reviews performance of internal control tasks at least annually.	Inspected the completed Security and Privacy Objectives to determine that the VP of Information Security reviewed performance of internal control tasks at least annually.	No exceptions noted.
		The Hosting team maintains procedures for operating, updating, and managing the production environment.	Inspected the hosting team policies and procedures to determine that the Hosting team maintained procedures for operating, updating, and managing the production environment.	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**
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Personnel are provided access to and required to review relevant company policies, code of conduct, and statement of confidentiality upon hire.	Inspected the company's intranet, the new hire onboarding e-mail, the onboarding and confidentiality acknowledgment for a sample of new hires, and the code of conduct acknowledgment for a sample of new hires to determine that personnel were provided access to and required to review relevant company policies, code of conduct, and statement of confidentiality upon hire.	No exceptions noted.
		Management monitors compliance with training requirements.	Inspected the training completion summary report to determine that management monitored compliance with training requirements.	No exceptions noted.
		Employee goals and objectives are used to frame performance evaluations.	Inquired of the Vice President of Information Security regarding the performance evaluation process to determine that employee goals and objectives were used to frame performance evaluations.	No exceptions noted.
			Inspected the employee performance review policy and the employee hub and manager review preparation sheet to determine that employee goals and objectives were used to frame performance evaluations.	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**
		A description of entity organizational structure, departmental functions, and employee resources is available to all employees on company intranet.	Inspected the company's intranet and the organizational chart to determine that a description of entity organizational structure, departmental functions, and employee resources was available to all employees on company intranet.	No exceptions noted.
		A reporting mechanism is in place to allow employees to report unethical behavior in a confidential manner.	Inspected the whistleblowing policy to determine that a reporting mechanism was in place to allow employees to report unethical behavior in a confidential manner.	No exceptions noted.
		Major changes to roles and responsibilities and changes to key personnel are communicated to relevant stakeholders.	Inspected the e-mail communication to stakeholders and companywide newsletters to determine that major changes to roles and responsibilities and changes to key personnel were communicated to relevant stakeholders.	No exceptions noted.
		Personnel are required to take an annual information security training.	Inquired of the Vice President of Information Security regarding the information security training to determine that personnel were required to take an annual information security training.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the information security training materials, the information security statement, and the completed information security training for a sample of current employees to determine that personnel were required to take an annual information security training.	No exceptions noted.
		Policies and procedures are documented for significant processes and are available on the entity's intranet.	Inspected the security documentation overview and the entity's intranet to determine that policies and procedures were documented for significant processes and were available on the entity's intranet.	No exceptions noted.
		Policy compliance is validated through internal audits, which are reviewed by management at least annually.	Inspected the completed internal audit results to determine that policy compliance was validated through internal audits and were reviewed by management at least annually.	No exceptions noted.
		Annual external penetration assessments are performed by an independent vendor as appropriate for client-facing applications.	Inspected the completed annual external penetration test to determine that annual external penetration assessments were performed by an independent vendor as appropriate for client-facing applications.	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.	The Company ensures its product designs provide capabilities for Clients and other interested parties to assess and enable or disable the impacts of AI features.	Inquired of the Governance, Risk and Compliance Manager regarding the AI capabilities to determine that the Company ensures its product designs provided capabilities for Clients and other interested parties to access and enable or disable the impacts of AI features.	No exceptions noted.
			Inspected the AI design procedures within the secure software development policy, the AI policy, the AI matrix, and the AI client configurations to determine that the Company ensures its product designs provided capabilities for Clients and other interested parties to access and enable or disable the impacts of AI features.	No exceptions noted.
		Company communicates to customers how to report operational failures, incidents, problems, concerns and complaints via the customer support portal.	Inspected the customer support portal and the customer support overview documentation to determine that the company communicated to customers how to report operational failures, incidents, problems, concerns and complaints via the customer support portal.	No exceptions noted.
		Major product releases are communicated to customers.	Inspected the customer release communication on the entity's website to determine that major product releases were communicated to customers.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company's security, availability, and confidentiality commitments regarding the system are included in customer contracts.	Inspected the customer contract master agreement template and the executed customer contract for a sample of customers to determine that the company's security, availability, and confidentiality commitments regarding the system were included in customer contracts.	No exceptions noted.
		System documentation is available to customers via a customer support portal.	Inspected the customer support portal to determine that the system documentation was available to customers via a customer support portal.	No exceptions noted.
		Major changes to roles and responsibilities and changes to key personnel are communicated to relevant stakeholders.	Inspected the e-mail communication to stakeholders and companywide newsletters to determine that major changes to roles and responsibilities and changes to key personnel were communicated to relevant stakeholders.	No exceptions noted.
		The entity has a defined process for assessing the adequacy and effectiveness of vendor controls.	Inspected the vendor management policy to determine that the entity has a defined process for assessing the adequacy and effectiveness of vendor controls.	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's third-party agreements outline and communicate the terms, conditions and responsibilities of third-parties.	Inspected the entity's third-party master template agreements and the executed third-party agreement for a sample of current third-parties and a sample of new third-parties to determine that the entity's third-party agreements outline and communicated the terms, conditions and responsibilities of third-parties.	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 organization shall define and enforce the policy for the responsible use of AI systems.	Inspected the AI policy, the AI policy acknowledgements for a sample of current employees, and the AI complaints and misuse tracker to determine that the organization shall define and enforce the policy for the responsible use of AI systems.	No exceptions noted.
		The Company identifies, documents, and assesses uses of AI systems within the organization.	Inspected the AI systems and inventory tracker to determine that the Company identified, documented, and assessed uses of AI systems within the organization.	No exceptions noted.
		The entity communicates organizational strategies and objectives to employees.	Inspected the entity's business update e-mails and newsletters to determine that the entity communicated organizational strategies and objectives to employees.	No exceptions noted.
		The entity monitors changes in laws and regulations and assesses their applicability to the business at least annually.	Inspected the completed legislation tracker, the legal counsel presentation related to the relevant statutory, regulatory, legislative and contractual requirements and the meeting invite to determine that the entity monitored changes in laws and regulations and assessed their applicability to the business at least annually.	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 has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policy and the completed risk assessment to determine that the entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		Executive Security Steering Committee meetings are held quarterly for Management to guide and review security and internal control objectives and performance.	Inspected the Executive Security Steering Committee meetings for a sample of quarters to determine that Executive Security Steering Committee meetings were held quarterly for Management to guide and review security and internal control objectives and performance.	No exceptions noted.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The Company identifies, documents, and assesses uses of AI systems within the organization.	Inspected the AI systems and inventory tracker to determine that the Company identified, documented, and assessed uses of AI systems within the organization.	No exceptions noted.
		The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policy and the completed risk assessment to determine that the entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	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 performs an annual risk assessment process to mitigate, remediate, or accept risks to the organization including vendor and fraud risks.	Inspected the completed risk assessment to determine that the entity performed an annual risk assessment process to mitigate, remediate, or accept risks to the organization including vendor and fraud risks.	No exceptions noted.
		The entity has a defined process for assessing the adequacy and effectiveness of vendor controls.	Inspected the vendor management policy to determine that the entity has a defined process for assessing the adequacy and effectiveness of vendor controls.	No exceptions noted.
		The entity's third-party agreements outline and communicate the terms, conditions and responsibilities of third-parties.	Inspected the entity's third-party master template agreements and the executed third-party agreement for a sample of current third-parties and a sample of new third-parties to determine that the entity's third-party agreements outline and communicated the terms, conditions and responsibilities of third-parties.	No exceptions noted.
		The entity qualifies and performs initial and thereafter annual risk assessments for its vendors.	Inquired of the Governance, Risk and Compliance Analyst regarding vendor management to determine that the entity qualified and performed initial and thereafter annual risk assessments for its 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**
			Inspected the vendor management policy, the completed vendor risk assessment, and the completed vendor risk assessment for a sample of new and existing vendors to determine that the entity qualified and performed initial and thereafter annual risk assessments for its vendors.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The entity performs an annual risk assessment process to mitigate, remediate, or accept risks to the organization including vendor and fraud risks.	Inspected the completed risk assessment to determine that the entity performed an annual risk assessment process to mitigate, remediate, or accept risks to the organization including vendor and fraud risks.	No exceptions noted.
		Fraud risks are evaluated on an annual basis including financial fraud risk and risk of fraud through the use of IT assets.	Inspected the completed risk assessment to determine that fraud risks were evaluated on an annual basis including financial fraud risk and risk of fraud through the use of IT assets.	No exceptions noted.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The entity has defined change management policies and procedures for systems.	Inspected the change management policy to determine that the entity has defined change management policies and procedures for systems.	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**
		Low risk changes to systems require pre-authorization and moderate or high risk changes require approval by the change authority prior to implementation.	Inspected the change management policy and the supporting change ticket for a sample of system changes to determine that low risk changes to systems required pre-authorization and moderate or high-risk changes require approval by the change authority prior to implementation.	No exceptions noted.
		The entity monitors changes in laws and regulations and assesses their applicability to the business at least annually.	Inspected the completed legislation tracker, the legal counsel presentation related to the relevant statutory, regulatory, legislative and contractual requirements and the meeting invite to determine that the entity monitored changes in laws and regulations and assessed their applicability to the business at least annually.	No exceptions noted.
		The entity performs an annual risk assessment process to mitigate, remediate, or accept risks to the organization including vendor and fraud risks.	Inspected the completed risk assessment to determine that the entity performed an annual risk assessment process to mitigate, remediate, or accept risks to the organization including vendor and fraud risks.	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.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, the FIM configurations, the IDS configurations, and the firewall rulesets for the production environment to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		Operations and security personnel follow defined protocols for resolving and escalating reported events.	Inquired of the Vice President of Information Security regarding the security event incident response plan to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted.
			Inspected the security event incident response plan and the supporting event report for a sample of events to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	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 has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policy and the completed risk assessment to determine that the entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		Annual external penetration assessments are performed by an independent vendor as appropriate for client-facing applications.	Inspected the completed annual external penetration test to determine that annual external penetration assessments were performed by an independent vendor as appropriate for client-facing applications.	No exceptions noted.
		The entity has a defined process for assessing the adequacy and effectiveness of vendor controls.	Inspected the vendor management policy to determine that the entity has a defined process for assessing the adequacy and effectiveness of vendor controls.	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.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, the FIM configurations, the IDS configurations, and the firewall rulesets for the production environment to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	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 has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policy and the completed risk assessment to determine that the entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		Risk treatments identified from the annual risk assessment are communicated to those parties responsible for taking corrective actions.	Inspected the completed risk assessment, the completed internal audit, and the supporting incident ticket for a sample of internal controls that had failed to determine that risk treatments identified from the annual risk assessment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
		Executive Security Steering Committee meetings are held quarterly for Management to guide and review security and internal control objectives and performance.	Inspected the Executive Security Steering Committee meetings for a sample of quarters to determine that Executive Security Steering Committee meetings were held quarterly for Management to guide and review security and internal control objectives and performance.	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 has a defined process for identifying, assessing, and remediating system vulnerabilities.	Inspected the vulnerability management policy, the supporting incident ticket for a sample of vulnerabilities identified from an external penetration test, and the supporting incident ticket for a sample of vulnerabilities identified from an entity performed vulnerability scan to determine that the entity has a defined process for identifying, assessing, and remediating system vulnerabilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Disaster recovery plans are developed and then updated and tested on at least an annual basis.	Inspected the business continuity planning and disaster recovery policy and the completed disaster recovery test results to determine that disaster recovery plans were developed and then updated and tested on at least an annual basis.	No exceptions noted.
		The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policy and the completed risk assessment to determine that the entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		The Company reviews the control environment during the annual risk assessment to determine whether its controls need to be added, modified, or removed.	Inspected the completed risk assessment, the completed security and privacy objectives, and the Executive Security Steering Committee meeting minutes to determine that the Company reviewed the control environment during the annual risk assessment to determine whether its controls need to be added, modified, or removed.	No exceptions noted.
		The VP of Information Security reviews performance of internal control tasks at least annually.	Inspected the completed Security and Privacy Objectives to determine that the VP of Information Security reviewed performance of internal control tasks at least annually.	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**
		Annual external penetration assessments are performed by an independent vendor as appropriate for client-facing applications.	Inspected the completed annual external penetration test to determine that annual external penetration assessments were performed by an independent vendor as appropriate for client-facing applications.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The Company's SDLC incorporates AI specific considerations to ensure that the systems are designed to implement AI related functionality in alignment with its principles.	Inspected the SDLC policy to determine that the Company's SDLC incorporates AI specific considerations to ensure that the systems were designed to implement AI related functionality in alignment with its principles.	No exceptions noted.
		Disaster recovery plans are developed and then updated and tested on at least an annual basis.	Inspected the business continuity planning and disaster recovery policy and the completed disaster recovery test results to determine that disaster recovery plans were developed and then updated and tested on at least an annual basis.	No exceptions noted.
		The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policy and the completed risk assessment to determine that the entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	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**
		Policies and procedures are documented for significant processes and are available on the entity's intranet.	Inspected the security documentation overview and the entity's intranet to determine that policies and procedures were documented for significant processes and were available on the entity's intranet.	No exceptions noted.
		Annual external penetration assessments are performed by an independent vendor as appropriate for client-facing applications.	Inspected the completed annual external penetration test to determine that annual external penetration assessments were performed by an independent vendor as appropriate for client-facing applications.	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Employee goals and objectives are used to frame performance evaluations.	Inquired of the Vice President of Information Security regarding the performance evaluation process to determine that employee goals and objectives were used to frame performance evaluations.	No exceptions noted.
			Inspected the employee performance review policy and the employee hub and manager review preparation sheet to determine that employee goals and objectives were used to frame performance evaluations.	No exceptions noted.
		Policies and procedures are documented for significant processes and are available on the entity's intranet.	Inspected the security documentation overview and the entity's intranet to determine that policies and procedures were documented for significant processes and were available on the entity's intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company reviews the control environment during the annual risk assessment to determine whether its controls need to be added, modified, or removed.	Inspected the completed risk assessment, the completed security and privacy objectives, and the Executive Security Steering Committee meeting minutes to determine that the Company reviewed the control environment during the annual risk assessment to determine whether its controls need to be added, modified, or removed.	No exceptions noted.
		The VP of Information Security reviews performance of internal control tasks at least annually.	Inspected the completed Security and Privacy Objectives to determine that the VP of Information Security reviewed performance of internal control tasks at least annually.	No exceptions noted.
		Policy compliance is validated through internal audits, which are reviewed by management at least annually.	Inspected the completed internal audit results to determine that policy compliance was validated through internal audits and were reviewed by management at least annually.	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.	Access to Hosting infrastructure requires privileged authentication credentials that are managed separately from the credentials for normal corporate users.	Inquired of the Vice President of Information Security regarding access to hosting infrastructure to determine that access to Hosting infrastructure requires privileged authentication credentials that were managed separately from the credentials for normal corporate users.	No exceptions noted.
			Observed the Vice President of Hosting Systems and Operations access the hosting infrastructure to determine that access to Hosting infrastructure requires privileged authentication credentials that were managed separately from the credentials for normal corporate users.	No exceptions noted.
			Inspected the access rights to hosting infrastructure to determine that access to Hosting infrastructure requires privileged authentication credentials that were managed separately from the credentials for normal corporate users.	No exceptions noted.
		A role-based security process has been defined with an access control system that is required to use roles where access is granted on an as-needed basis.	Inquired of the Vice President of Information Security regarding role-based security access control to determine that a role-based security process has been defined with an access control system that was required to use roles where access was granted on an as-needed basis.	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 access management policy and the hosted user listing and access rights to determine that a role-based security process has been defined with an access control system that was required to use roles where access was granted on an as-needed basis.	No exceptions noted.
		VPN access is restricted to authorized personnel.	Inquired of the Governance, Risk, and Compliance Manager regarding VPN access to determine that VPN access was restricted to authorized personnel.	No exceptions noted.
			Inspected the VPN user listing to determine that VPN access was restricted to authorized personnel.	No exceptions noted.
		Access to production environment jump boxes, bastion hosts, or other access restriction methodologies is restricted to authorized users in a security group.	Inquired of the Vice President of Information Security regarding production access jump boxes to determine that access to the production environment jump boxes, bastion hosts, or other access restriction methodologies was restricted to authorized users in a security group.	No exceptions noted.
			Observed the Vice President of Hosting Systems and Operations access the jump boxes to determine that access to the production environment jump boxes, bastion hosts, or other access restriction methodologies was restricted to authorized users in a security group.	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 production security group and the production user listings to determine that access to the production environment jump boxes, bastion hosts, or other access restriction methodologies was restricted to authorized users in a security group.	No exceptions noted.
		Security attributes are granted on the principle of least privilege.	Inspected the application access helper guide and an example supporting cloud security access request ticket to determine that security attributes were granted on the principle of least privilege.	No exceptions noted.
		Company defines and enforces password strength best practices through policy and configurations.	Inspected the password policy and the password configuration to determine that company defines and enforced password strength best practices through policy and configurations.	No exceptions noted.
		Multifactor authentication is enforced for remote access.	Inquired of the Vice President of Information Security regarding multifactor authentication to determine that multifactor authentication was enforced for remote access.	No exceptions noted.
			Observed the Vice President of Hosting Systems and Operations access the hosting environment to determine that multifactor authentication was enforced for remote access.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the multifactor configurations to determine that multifactor authentication was enforced for remote access.	No exceptions noted.
		Stored passwords in applications and for infrastructure components are encrypted.	Inspected the password vault tool and the password encryption configurations for applications, the data encryption policy and the data classification and handling policy to determine that stored passwords in applications and for infrastructure components were encrypted.	No exceptions noted.
		The entity has defined system and configuration hardening standards.	Inspected the system hardening configuration standards to determine that the entity has a defined system and configuration hardening standards.	No exceptions noted.
		SaaS system architecture is reviewed for security best practices on a monthly basis.	Inspected the SaaS system architecture review meeting minutes for a sample of months to determine that the entity's system architecture was reviewed for security best practices on a monthly basis.	No exceptions noted.
		Logging is configured to support investigatory and forensic purposes.	Inquired of the Vice President of Information Security regarding audit logs to determine that logging was configured to support investigatory and forensic purposes.	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 security information and event management (SIEM) Procedures and the Center for Information Security (CIS) Benchmark assessments monitoring procedures and the central log monitoring configurations for the internal network, the production network operating systems, the databases, the applications and the VPN to determine that logging was configured to support investigatory and forensic purposes.	No exceptions noted.
		Customer data is isolated through network segmentation and access controls.	Inquired of the Vice President of Information Security regarding customer data to determine that customer data was isolated through network segmentation and access controls.	No exceptions noted.
			Inspected the network diagrams, the network segmentation, and the user access listings to determine that customer data was isolated through network segmentation and access controls.	No exceptions noted.
		External access is controlled by firewalls and access control lists.	Inspected the security baseline policy, the user access listings, the network diagrams and the firewall rulesets for the production environment to determine that external access was controlled by firewalls and access control lists.	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**
		Annual external penetration assessments are performed by an independent vendor as appropriate for client-facing applications.	Inspected the completed annual external penetration test to determine that annual external penetration assessments were performed by an independent vendor as appropriate for client-facing applications.	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.
CC6.2	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.	New access is approved and granted as part of the new hire onboarding process.	Inquired of the Vice President of Information Security regarding the new access for new hires to determine that new access was approved and granted as part of the new hire onboarding process.	No exceptions noted.
			Inspected the IT New Starter Process, the user access listings and the supporting hiring user access request ticket for a sample of new hires to determine that new access was approved and granted as part of the new hire onboarding process.	No exceptions noted.
		Upon termination, system access is removed.	Inquired of the Governance, Risk, and Compliance Manager regarding the terminated access policies and procedures to determine that upon termination, system access was removed.	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 IT leavers process, the deprovisioning procedure, the system user access listings and the supporting terminated user access revocation ticket for a sample of terminated employees to determine that upon termination, system access was removed.	No exceptions noted.
		Credentials for Privileged Access to SaaS environments are changed at least annually.	Inquired of the Vice President of Information Security regarding privileged access to determine that credentials for privileged access to SaaS environments were changed at least annually.	No exceptions noted.
			Inspected the SaaS password policy and the SaaS password configuration to determine that credentials for privileged access to SaaS environments were changed at least annually.	No exceptions noted.
		Named user accounts are required when supported by a service.	Inquired of the Vice President of Information Security regarding named user accounts to determine that named user accounts were required when supported by a service.	No exceptions noted.
			Observed the Vice President of Hosting Systems and Operations access the production servers to determine that named user accounts were required when supported by a service.	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 named user accounts to determine that named user accounts were required when supported by a service.	No exceptions noted.
		Production access reviews occur on a quarterly basis.	Inquired of the Governance, Risk, and Compliance Manager regarding the production access reviews for a sample of quarters to determine that production access reviews occurred on a quarterly basis.	No exceptions noted.
			Inspected the production access reviews for a sample of quarters to determine that production access reviews occurred on a quarterly basis.	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.	New access is approved and granted as part of the new hire onboarding process.	Inquired of the Vice President of Information Security regarding the new access for new hires to determine that new access was approved and granted as part of the new hire onboarding process.	No exceptions noted.
			Inspected the IT New Starter Process, the user access listings and the supporting hiring user access request ticket for a sample of new hires to determine that new access was approved and granted as part of the new hire onboarding 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**
		Upon termination, system access is removed.	Inquired of the Governance, Risk, and Compliance Manager regarding the terminated access policies and procedures to determine that upon termination, system access was removed.	No exceptions noted.
			Inspected the IT leavers process, the deprovisioning procedure, the system user access listings and the supporting terminated user access revocation ticket for a sample of terminated employees to determine that upon termination, system access was removed.	No exceptions noted.
		Credentials for Privileged Access to SaaS environments are changed at least annually.	Inquired of the Vice President of Information Security regarding privileged access to determine that credentials for privileged access to SaaS environments were changed at least annually.	No exceptions noted.
			Inspected the SaaS password policy and the SaaS password configuration to determine that credentials for privileged access to SaaS environments were changed at least annually.	No exceptions noted.
		Named user accounts are required when supported by a service.	Inquired of the Vice President of Information Security regarding named user accounts to determine that named user accounts were required when supported by a service.	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**
			Observed the Vice President of Hosting Systems and Operations access the production servers to determine that named user accounts were required when supported by a service.	No exceptions noted.
			Inspected the listings of named user accounts to determine that named user accounts were required when supported by a service.	No exceptions noted.
		Production access reviews occur on a quarterly basis.	Inquired of the Governance, Risk, and Compliance Manager regarding the production access reviews for a sample of quarters to determine that production access reviews occurred on a quarterly basis.	No exceptions noted.
			Inspected the production access reviews for a sample of quarters to determine that production access reviews occurred on a quarterly basis.	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**
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Policies and procedures are in place to guide personnel in data, hardware and software erasure, disposal or destruction.	Inquired of the Vice President of Information Security regarding the data retention, destruction, and hardware disposal policy to determine that policies and procedures were in place to guide personnel in data, hardware and software erasure, disposal or destruction.	No exceptions noted.
			Inspected the data retention, destruction and disposal policy and the destruction certificate for a sample of requests to dispose of data, purge a system, or physically destroy a system to determine that policies and procedures were in place to guide personnel in data, hardware and software erasure, disposal or destruction.	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**
		Customer data is removed in a timely manner at the end of a contract.	Inspected the customer data disposal and destruction policies and procedures within the data retention, destruction and disposal policy and procedures and the supporting service ticket for a sample of requests to dispose of data from a customer to determine that customer data was removed in a timely manner at the end of a contract.	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.	Client data is encrypted in transit and at rest using Transport Layer Security (TLS) or other certificate based encryption.	Inspected the encryption configurations to determine that client data was encrypted in transit and at rest using TLS or other certificate based encryption.	No exceptions noted.
		Multifactor authentication is enforced for remote access.	Inquired of the Vice President of Information Security regarding multifactor authentication to determine that multifactor authentication was enforced for remote access.	No exceptions noted.
			Observed the Vice President of Hosting Systems and Operations access the hosting environment to determine that multifactor authentication was enforced for remote access.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the multifactor configurations to determine that multifactor authentication was enforced for remote access.	No exceptions noted.
		External access is controlled by firewalls and access control lists.	Inspected the security baseline policy, the user access listings, the network diagrams and the firewall rulesets for the production environment to determine that external access was controlled by firewalls and access control lists.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and the firewall rulesets for the production environment to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Software is deployed to protect against virus, malware, ransomware and similar attacks.	Inspected the antivirus policies within the security baselines policy, the antivirus software dashboard console, the antivirus software configurations for a sample of servers, and the antivirus software configurations for a sample of workstations to determine that software was deployed to protect against virus, malware, ransomware and similar attacks.	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**
		Use of removable media is prohibited except when authorized by management.	Inspected the acceptable use policy and the removable media configurations to determine that use of removable media was prohibited except when authorized by management.	No exceptions noted.
		IDS are in place to analyze and prevent network security breaches.	Inspected the IDS configurations to determine that an IDS was in place to analyze and prevent network security breaches.	No exceptions noted.
		Detected security events generate notifications and alert personnel.	Inspected the cloud security configurations and an example cloud security alert to determine that detected security events generate notifications and alert personnel.	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.
CC6.7	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.	Entity policies prohibit the transmission of sensitive information over the internet or other public communications paths unless it is encrypted.	Inspected the data classification and handling policy and the data encryption policy to determine that entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted.	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**
		Multifactor authentication is enforced for remote access.	Inquired of the Vice President of Information Security regarding multifactor authentication to determine that multifactor authentication was enforced for remote access.	No exceptions noted.
			Observed the Vice President of Hosting Systems and Operations access the hosting environment to determine that multifactor authentication was enforced for remote access.	No exceptions noted.
			Inspected the multifactor configurations to determine that multifactor authentication was enforced for remote access.	No exceptions noted.
		End user devices are centrally managed and applicable secure configuration standards are enforced	Inspected the security baseline policy and the centralized end user device management configurations to determine that end user devices were centrally managed and applicable secure configuration standards were enforced.	No exceptions noted.
		Client data is encrypted in transit and at rest using Transport Layer Security (TLS) or other certificate based encryption.	Inspected the encryption configurations to determine that client data was encrypted in transit and at rest using TLS or other certificate based encryption.	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.	VPN access is restricted to authorized personnel.	Inquired of the Governance, Risk, and Compliance Manager regarding VPN access to determine that VPN access was restricted to authorized personnel.	No exceptions noted.
			Inspected the VPN user listing to determine that VPN access was restricted to authorized personnel.	No exceptions noted.
		Access to production environment jump boxes, bastion hosts, or other access restriction methodologies is restricted to authorized users in a security group.	Inquired of the Vice President of Information Security regarding production access jump boxes to determine that access to the production environment jump boxes, bastion hosts, or other access restriction methodologies was restricted to authorized users in a security group.	No exceptions noted.
			Observed the Vice President of Hosting Systems and Operations access the jump boxes to determine that access to the production environment jump boxes, bastion hosts, or other access restriction methodologies was restricted to authorized users in a security group.	No exceptions noted.
			Inspected the production security group and the production user listings to determine that access to the production environment jump boxes, bastion hosts, or other access restriction methodologies was restricted to authorized users in a security group.	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**
		Security attributes are granted on the principle of least privilege.	Inspected the application access helper guide and an example supporting cloud security access request ticket to determine that security attributes were granted on the principle of least privilege.	No exceptions noted.
		Software is deployed to protect against virus, malware, ransomware and similar attacks.	Inspected the antivirus policies within the security baselines policy, the antivirus software dashboard console, the antivirus software configurations for a sample of servers, and the antivirus software configurations for a sample of workstations to determine that software was deployed to protect against virus, malware, ransomware and similar attacks.	No exceptions noted.
		IDS are in place to analyze and prevent network security breaches.	Inspected the IDS configurations to determine that an IDS was in place to analyze and prevent network security breaches.	No exceptions noted.
		Detected security events generate notifications and alert personnel.	Inspected the cloud security configurations and an example cloud security alert to determine that detected security events generate notifications and alert personnel.	No exceptions noted.
		Annual external penetration assessments are performed by an independent vendor as appropriate for client-facing applications.	Inspected the completed annual external penetration test to determine that annual external penetration assessments were performed by an independent vendor as appropriate for client-facing applications.	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.

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.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, the FIM configurations, the IDS configurations, and the firewall rulesets for the production environment to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		Policies and procedures are documented for significant processes and are available on the entity's intranet.	Inspected the security documentation overview and the entity's intranet to determine that policies and procedures were documented for significant processes and were available on the entity's intranet.	No exceptions noted.
		The entity has defined system and configuration hardening standards.	Inspected the system hardening configuration standards to determine that the entity has a defined system and configuration hardening standards.	No exceptions noted.
		IDS are in place to analyze and prevent network security breaches.	Inspected the IDS configurations to determine that an IDS was in place to analyze and prevent network security breaches.	No exceptions noted.
		Detected security events generate notifications and alert personnel.	Inspected the cloud security configurations and an example cloud security alert to determine that detected security events generate notifications and alert personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Annual external penetration assessments are performed by an independent vendor as appropriate for client-facing applications.	Inspected the completed annual external penetration test to determine that annual external penetration assessments were performed by an independent vendor as appropriate for client-facing applications.	No exceptions noted.
		The entity performs testing at least annually to detect vulnerabilities in its client systems and configurations.	Inspected the completed entity vulnerability scan results, the management meetings for a sample of months and the supporting vulnerability ticket for a sample of vulnerabilities identified from an entity performed vulnerability scan to determine that the entity performed testing at least annually to detect vulnerabilities in its client systems and configurations.	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**
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, the FIM configurations, the IDS configurations, and the firewall rulesets for the production environment to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		Operations and security personnel follow defined protocols for resolving and escalating reported events.	Inquired of the Vice President of Information Security regarding the security event incident response plan to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted.
			Inspected the security event incident response plan and the supporting event report for a sample of events to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted.
		Disaster recovery plans are developed and then updated and tested on at least an annual basis.	Inspected the business continuity planning and disaster recovery policy and the completed disaster recovery test results to determine that disaster recovery plans were developed and then updated and tested on at least an annual basis.	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**
		Backups are evaluated to identify backup failures.	Inspected the data backup policy, the failed backup alerting configurations and the on-call how to documentations, and the supporting ticket for a sample of failed backups to determine that backups were evaluated to identify backup failures.	No exceptions noted.
		External access is controlled by firewalls and access control lists.	Inspected the security baseline policy, the user access listings, the network diagrams and the firewall rulesets for the production environment to determine that external access was controlled by firewalls and access control lists.	No exceptions noted.
		Software is deployed to protect against virus, malware, ransomware and similar attacks.	Inspected the antivirus policies within the security baselines policy, the antivirus software dashboard console, the antivirus software configurations for a sample of servers, and the antivirus software configurations for a sample of workstations to determine that software was deployed to protect against virus, malware, ransomware and similar attacks.	No exceptions noted.
		IDS are in place to analyze and prevent network security breaches.	Inspected the IDS configurations to determine that an IDS was in place to analyze and prevent network security breaches.	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**
		Detected security events generate notifications and alert personnel.	Inspected the cloud security configurations and an example cloud security alert to determine that detected security events generate notifications and alert personnel.	No exceptions noted.
		Logging is configured to support investigatory and forensic purposes.	Inquired of the Vice President of Information Security regarding audit logs to determine that logging was configured to support investigatory and forensic purposes.	No exceptions noted.
			Inspected the security information and event management (SIEM) Procedures and the Center for Information Security (CIS) Benchmark assessments monitoring procedures and the central log monitoring configurations for the internal network, the production network operating systems, the databases, the applications and the VPN to determine that logging was configured to support investigatory and forensic purposes.	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.	Company policies include corrective action and termination procedures for instances of misconduct or policy noncompliance.	Inspected the termination policy and disciplinary action policy documented within the code book to determine that company policies included corrective action and termination procedures for instances of misconduct or policy noncompliance.	No exceptions noted.
		Operations and security personnel follow defined protocols for resolving and escalating reported events.	Inquired of the Vice President of Information Security regarding the security event incident response plan to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted.
			Inspected the security event incident response plan and the supporting event report for a sample of events to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted.
		A defined incident response plan is in place that defines roles and responsibilities, and the process for engaging relevant stakeholders and managing the complete incident lifecycle, including documentation, communication, containment, resolution, and recover.	Inspected the security event incident response plan to determine that a defined incident response plan was in place that defines roles and responsibilities, and the process for engaging relevant stakeholders and managing the complete incident lifecycle, including documentation, communication, containment, resolution, and recovery.	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 entity performs a security table-top exercise or equivalent annually to test the security incident response plan.	Inspected the completed security incident tabletop exercise and the completion report to determine that the entity performed a security table-top exercise or equivalent annually to test the security incident response plan.	No exceptions noted.
		The entity performs an annual risk assessment process to mitigate, remediate, or accept risks to the organization including vendor and fraud risks.	Inspected the completed risk assessment to determine that the entity performed an annual risk assessment process to mitigate, remediate, or accept risks to the organization including vendor and fraud risks.	No exceptions noted.
		Risk treatments identified from the annual risk assessment are communicated to those parties responsible for taking corrective actions.	Inspected the completed risk assessment, the completed internal audit, and the supporting incident ticket for a sample of internal controls that had failed to determine that risk treatments identified from the annual risk assessment were communicated to those parties responsible for taking corrective actions.	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**
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Operations and security personnel follow defined protocols for resolving and escalating reported events.	Inquired of the Vice President of Information Security regarding the security event incident response plan to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted.
			Inspected the security event incident response plan and the supporting event report for a sample of events to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted.
		Disaster recovery plans are developed and then updated and tested on at least an annual basis.	Inspected the business continuity planning and disaster recovery policy and the completed disaster recovery test results to determine that disaster recovery plans were developed and then updated and tested on at least an annual basis.	No exceptions noted.
		A defined incident response plan is in place that defines roles and responsibilities, and the process for engaging relevant stakeholders and managing the complete incident lifecycle, including documentation, communication, containment, resolution, and recover.	Inspected the security event incident response plan to determine that a defined incident response plan was in place that defines roles and responsibilities, and the process for engaging relevant stakeholders and managing the complete incident lifecycle, including documentation, communication, containment, resolution, and recovery.	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 incident response plan is reviewed at least annually.	Inspected the security event incident response plan to determine that the security incident response plan was reviewed at least annually.	No exceptions noted.
		The entity performs a security table-top exercise or equivalent annually to test the security incident response plan.	Inspected the completed security incident tabletop exercise and the completion report to determine that the entity performed a security table-top exercise or equivalent annually to test the security incident response plan.	No exceptions noted.
		Prior to closing out an incident, a postmortem is performed, that includes analysis of root cause and continuous improvement opportunities.	Inquired of the Vice President of Information Security regarding postmortem activities to determine that prior to closing out an incident, a postmortem was performed, that included analysis of root cause and continuous improvement opportunities.	No exceptions noted.
			Inspected the security event incident response plan and the supporting postmortem documentation for a sample of events to determine that prior to closing out an incident, a postmortem was performed, that included analysis of root cause and continuous improvement opportunities.	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**
		Executive Security Steering Committee meetings are held quarterly for Management to guide and review security and internal control objectives and performance.	Inspected the Executive Security Steering Committee meetings for a sample of quarters to determine that Executive Security Steering Committee meetings were held quarterly for Management to guide and review security and internal control objectives and performance.	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.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Operations and security personnel follow defined protocols for resolving and escalating reported events.	Inquired of the Vice President of Information Security regarding the security event incident response plan to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted.
			Inspected the security event incident response plan and the supporting event report for a sample of events to determine that operations and security personnel followed defined protocols for resolving and escalating reported 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**
		Disaster recovery plans are developed and then updated and tested on at least an annual basis.	Inspected the business continuity planning and disaster recovery policy and the completed disaster recovery test results to determine that disaster recovery plans were developed and then updated and tested on at least an annual basis.	No exceptions noted.
		A defined incident response plan is in place that defines roles and responsibilities, and the process for engaging relevant stakeholders and managing the complete incident lifecycle, including documentation, communication, containment, resolution, and recover.	Inspected the security event incident response plan to determine that a defined incident response plan was in place that defines roles and responsibilities, and the process for engaging relevant stakeholders and managing the complete incident lifecycle, including documentation, communication, containment, resolution, and recovery.	No exceptions noted.
		The entity performs a security table-top exercise or equivalent annually to test the security incident response plan.	Inspected the completed security incident tabletop exercise and the completion report to determine that the entity performed a security table-top exercise or equivalent annually to test the security incident response plan.	No exceptions noted.
		Data is backed up daily to support recovery requirements.	Inspected the backup data policy and the backup configurations and an example log to determine that data was backed up daily to support recovery requirements.	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**
		Backups are evaluated to identify backup failures.	Inspected the data backup policy, the failed backup alerting configurations and the on-call how to documentations, and the supporting ticket for a sample of failed backups to determine that backups were evaluated to identify backup failures.	No exceptions noted.
		Backups are encrypted, rotated and safely segregated as an additional disaster recovery measure.	Inquired of the Vice President of Information Security regarding backup media encryption to determine that backup media was encrypted, rotated and safely segregated as an additional disaster recovery measure.	No exceptions noted.
			Inspected the contract in place with the backup storage vendor, the backup configurations for rotation and segregation, the backup media encryption configurations and the supporting ticket for a sample of data restorations to determine that backup media was encrypted, rotated and safely segregated as an additional disaster recovery measure.	No exceptions noted.
		Executive Security Steering Committee meetings are held quarterly for Management to guide and review security and internal control objectives and performance.	Inspected the Executive Security Steering Committee meetings for a sample of quarters to determine that Executive Security Steering Committee meetings were held quarterly for Management to guide and review security and internal control objectives and performance.	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**
		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				
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 role-based security process has been defined with an access control system that is required to use roles where access is granted on an as-needed basis.	Inquired of the Vice President of Information Security regarding role-based security access control to determine that a role-based security process has been defined with an access control system that was required to use roles where access was granted on an as-needed basis.	No exceptions noted.
			Inspected the access management policy and the hosted user listing and access rights to determine that a role-based security process has been defined with an access control system that was required to use roles where access was granted on an as-needed basis.	No exceptions noted.
		The entity has defined change management policies and procedures for systems.	Inspected the change management policy to determine that the entity has defined change management policies and procedures for systems.	No exceptions noted.
		Low risk changes to systems require pre-authorization and moderate or high risk changes require approval by the change authority prior to implementation.	Inspected the change management policy and the supporting change ticket for a sample of system changes to determine that low risk changes to systems required pre-authorization and moderate or high-risk changes require approval by the change authority prior to implementation.	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**
		A Production Change Authority is in place to review system change requests, including the potential effect on security, availability, and confidentiality commitments and requirements.	Inspected the change management policy and the production change board meeting attendance records for a sample of weeks to determine that a Production Change Authority was in place to review system change requests, including the potential effect on security, availability, and confidentiality commitments and requirements.	No exceptions noted.
		Change request tickets are reviewed by subject matter experts to ensure changes requested are appropriate, performed accurately and testing was conducted when necessary.	Inspected the supporting change ticket for a sample of system changes to determine that change request tickets were reviewed by subject matter experts to ensure changes requested were appropriate, performed accurately and testing was conducted when necessary.	No exceptions noted.
		Company communicates to customers how to report operational failures, incidents, problems, concerns and complaints via the customer support portal.	Inspected the customer support portal and the customer support overview documentation to determine that the company communicated to customers how to report operational failures, incidents, problems, concerns and complaints via the customer support portal.	No exceptions noted.
		Major product releases are communicated to customers.	Inspected the customer release communication on the entity's website to determine that major product releases were communicated to customers.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Company prohibits the use of Production data in test environments.	Inspected the client data access and manipulation policy within the data classification and handling policy, the secure software development policy, and the data anonymizing script for the test environment to determine that the company prohibited the use of production data in test environments.	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				
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 entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the risk management policy and the completed risk assessment to determine that the entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
		The entity performs an annual risk assessment process to mitigate, remediate, or accept risks to the organization including vendor and fraud risks.	Inspected the completed risk assessment to determine that the entity performed an annual risk assessment process to mitigate, remediate, or accept risks to the organization including vendor and fraud risks.	No exceptions noted.
		Risk treatments identified from the annual risk assessment are communicated to those parties responsible for taking corrective actions.	Inspected the completed risk assessment, the completed internal audit, and the supporting incident ticket for a sample of internal controls that had failed to determine that risk treatments identified from the annual risk assessment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
		Fraud risks are evaluated on an annual basis including financial fraud risk and risk of fraud through the use of IT assets.	Inspected the completed risk assessment to determine that fraud risks were evaluated on an annual basis including financial fraud risk and risk of fraud through the use of IT assets.	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**
		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.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The Company's vendor management process includes assessment of AI considerations for relevant vendors.	Inspected the vendor management policy, the AI policy, and the completed vendor risk assessment to determine that the company's vendor management process includes assessment of AI considerations for relevant vendors.	No exceptions noted.
		The entity has a defined process for assessing the adequacy and effectiveness of vendor controls.	Inspected the vendor management policy to determine that the entity has a defined process for assessing the adequacy and effectiveness of vendor controls.	No exceptions noted.
		The entity's third-party agreements outline and communicate the terms, conditions and responsibilities of third-parties.	Inspected the entity’s third-party master template agreements and the executed third-party agreement for a sample of current third-parties and a sample of new third-parties to determine that the entity’s third-party agreements outline and communicated the terms, conditions and responsibilities of third-parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity qualifies and performs initial and thereafter annual risk assessments for its vendors.	Inquired of the Governance, Risk and Compliance Analyst regarding vendor management to determine that the entity qualified and performed initial and thereafter annual risk assessments for its vendors.	No exceptions noted.
			Inspected the vendor management policy, the completed vendor risk assessment, and the completed vendor risk assessment for a sample of new and existing vendors to determine that the entity qualified and performed initial and thereafter annual risk assessments for its vendors.	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.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, the FIM configurations, the IDS configurations, and the firewall rulesets for the production environment to determine that monitoring software was used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		Operations and security personnel follow defined protocols for resolving and escalating reported events.	Inquired of the Vice President of Information Security regarding the security event incident response plan to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted.
			Inspected the security event incident response plan and the supporting event report for a sample of events to determine that operations and security personnel followed defined protocols for resolving and escalating reported events.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Resources that can be scaled dynamically are configured to do so, and otherwise resource pools are made available as necessary to accommodate changing static capacity needs.	Inspected the auto scaling and resource pool configurations, the budget review meeting minutes for security, and the security council meeting minutes for a sample of months to determine that resources that can be scaled dynamically were configured to do so, and otherwise resource pools were made available as necessary to accommodate changing static capacity needs.	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.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Data is backed up daily to support recovery requirements.	Inspected the backup data policy and the backup configurations and an example log to determine that data was backed up daily to support recovery requirements.	No exceptions noted.
		Backups are evaluated to identify backup failures.	Inspected the data backup policy, the failed backup alerting configurations and the on-call how to documentations, and the supporting ticket for a sample of failed backups to determine that backups were evaluated to identify backup failures.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Backups are encrypted, rotated and safely segregated as an additional disaster recovery measure.	Inquired of the Vice President of Information Security regarding backup media encryption to determine that backup media was encrypted, rotated and safely segregated as an additional disaster recovery measure.	No exceptions noted.
			Inspected the contract in place with the backup storage vendor, the backup configurations for rotation and segregation, the backup media encryption configurations and the supporting ticket for a sample of data restorations to determine that backup media was encrypted, rotated and safely segregated as an additional disaster recovery measure.	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.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Disaster recovery plans are developed and then updated and tested on at least an annual basis.	Inspected the business continuity planning and disaster recovery policy and the completed disaster recovery test results to determine that disaster recovery plans were developed and then updated and tested on at least an annual basis.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity performs a security table-top exercise or equivalent annually to test the security incident response plan.	Inspected the completed security incident tabletop exercise and the completion report to determine that the entity performed a security table-top exercise or equivalent annually to test the security incident response plan.	No exceptions noted.
		Backups are evaluated to identify backup failures.	Inspected the data backup policy, the failed backup alerting configurations and the on-call how to documentations, and the supporting ticket for a sample of failed backups to determine that backups were evaluated to identify backup failures.	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.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	VPN access is restricted to authorized personnel.	Inquired of the Governance, Risk, and Compliance Manager regarding VPN access to determine that VPN access was restricted to authorized personnel.	No exceptions noted.
			Inspected the VPN user listing to determine that VPN access was restricted to authorized personnel.	No exceptions noted.
		Access to production environment jump boxes, bastion hosts, or other access restriction methodologies is restricted to authorized users in a security group.	Inquired of the Vice President of Information Security regarding production access jump boxes to determine that access to the production environment jump boxes, bastion hosts, or other access restriction methodologies was restricted to authorized users in a security group.	No exceptions noted.
			Observed the Vice President of Hosting Systems and Operations access the jump boxes to determine that access to the production environment jump boxes, bastion hosts, or other access restriction methodologies was restricted to authorized users in a security group.	No exceptions noted.
			Inspected the production security group and the production user listings to determine that access to the production environment jump boxes, bastion hosts, or other access restriction methodologies was restricted to authorized users in a security group.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Security attributes are granted on the principle of least privilege.	Inspected the application access helper guide and an example supporting cloud security access request ticket to determine that security attributes were granted on the principle of least privilege.	No exceptions noted.
		Entity policies prohibit the transmission of sensitive information over the internet or other public communications paths unless it is encrypted.	Inspected the data classification and handling policy and the data encryption policy to determine that entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted.	No exceptions noted.
		The Company prohibits the use of Production data in test environments.	Inspected the client data access and manipulation policy within the data classification and handling policy, the secure software development policy, and the data anonymizing script for the test environment to determine that the company prohibited the use of production data in test environments.	No exceptions noted.
		Hosted products are designed to support multiple levels of access.	Inspected the levels of access to determine that hosted products were designed to support multiple levels of access.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Policies and procedures are in place to guide personnel in data, hardware and software erasure, disposal or destruction.	Inquired of the Vice President of Information Security regarding the data retention, destruction, and hardware disposal policy to determine that policies and procedures were in place to guide personnel in data, hardware and software erasure, disposal or destruction.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the data retention, destruction and disposal policy and the destruction certificate for a sample of requests to dispose of data, purge a system, or physically destroy a system to determine that policies and procedures were in place to guide personnel in data, hardware and software erasure, disposal or destruction.	No exceptions noted.
		Customer data is removed in a timely manner at the end of a contract.	Inspected the customer data disposal and destruction policies and procedures within the data retention, destruction and disposal policy and procedures and the supporting service ticket for a sample of requests to dispose of data from a customer to determine that customer data was removed in a timely manner at the end of a contract.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
CC1.1, CC1.3, CC1.4, CC1.5	Performance reviews are performed at least annually.	Inspected the performance evaluation form for a sample of current employees to determine that performance reviews were performed at least annually.	Testing of the control activity disclosed that a performance review was not performed on an annual basis for two of 40 current employees sampled.	One of the two sampled reviews was missed due to an administrative oversight resulting from organizational change; the other was due to a delay in completing the review before the review cycle was closed. Management has since strengthened the compliance oversight of this process to ensure that sufficient follow-up occurs during review cycles to prevent missed reviews or delays exceeding the cycle end date.