TSG GLOBAL, INC

SOC 2® Report

Type 2

Controls Relevant to Security

For the Period April 3, 2022 to April 2, 2023

Prepared in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA)

MJD ADVISORS

AICPA SOC aicpa.org/soc4so SOC for Service Organizations ™

Table of Contents

Section 1

Independent Service Auditor's Report

Independent Service Auditor's Report

To the Management of TSG Global, Inc
Holbrook, Massachusetts

Scope

We have examined TSG Global, Inc's (the Company) accompanying description in Section 3 titled "Management's Description of the TSG Platform" throughout the period April 3, 2022 to April 2, 2023 (description) based on the criteria for a description of a service organization's system set forth in DC 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 3, 2022 to April 2, 2023, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

Service Organization's Responsibilities

The Company is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to ensure the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion in Section 2 titled "Assertion of TSG Global, Inc Management" (assertion) about the description and suitability of the design and operating effectiveness of controls. The Company 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 the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted following attestation standards established by the AICPA. Those standards require 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 whether the controls stated were suitably designed and operating effectively to provide reasonable assurance the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

We believe the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion. We are required to be independent of the Company and to meet our other responsibilities in accordance with relevant ethical requirements relating to the engagement.

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

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in the accompanying "Information Provided by Service Auditor" in Section 4.

Opinion

In our opinion, in all material respects:

a) The description presents the TSG Platform that was designed and implemented throughout the period April 3, 2022 to April 2, 2023, in accordance with the description criteria.

b) The controls stated in the description were suitably designed throughout the period April 3, 2022 to April 2, 2023, to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout the period and if the subservice organizations applied the complementary controls assumed in the design of the Company's controls throughout the period.

c) The controls stated in the description operated effectively throughout the period April 3, 2022 to April 2, 2023, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of the Company'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 the Company, user entities of the TSG Platform during some or all of the period April 3, 2022 to April 2, 2023, business partners of the Company subject to risks arising from interactions with the TSG Platform, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to 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 the specified parties.

MJD Advisors

Waukee, Iowa
May 22, 2023

Section 2

Management's Assertion

Assertion of TSG Global, Inc Management

Management of TSG Global, Inc has prepared the accompanying description titled "Management's Description of the TSG Platform" throughout the period April 3, 2022, to April 2, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*). The description is intended to provide report users with information about the TSG Platform that may be useful when assessing the risks arising from interactions with the TSG Platform, particularly information about system controls the Company 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 set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The Company uses a subservice organization to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Company's controls. The description does not disclose the actual controls at the subservice organization.

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

a) The description presents the TSG Platform that was designed and implemented throughout the period April 3, 2022, to April 2, 2023, in accordance with the description criteria.

b) The controls stated in the description were suitably designed throughout the period April 3, 2022, to April 2, 2023, to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout the period April 3, 2022, to April 2, 2023, and if the subservice organizations applied the complementary controls assumed in the design of the Company's controls throughout the period April 3, 2022, to April 2, 2023.

c) The controls stated in the description operated effectively throughout the period April 3, 2022, to April 2, 2023, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of the Company's controls operated effectively throughout that period.

Management of TSG Global, Inc
May 22, 2023

Section 3

System Description

System Description

Management's Description of the TSG Platform
For the Period April 3, 2022 to April 2, 2023

Types of Services Provided

TSG Global, Inc. was founded in 2006 to help software-as-a-service (SaaS) and enterprise clients solve their current and future communication needs and requirements. The TSG Platform (the Platform) was developed to give its clients greater control over their telecommunications ecosystem, enabling them to manage multiple carriers by leveraging a flexible and powerful transaction settlement engine. The Platform can design and deploy multiple aspects of the client's communication portfolio, including text messaging and voice, and perform migration and porting via electronic Letter of Authorization.

The Platform is hosted on a cloud computing infrastructure and connects with clients via Short Message Peer-to-Peer (SMPP), Session Initiation Protocol (SIP), and representational state transfer (REST) or GraphQL application programming interfaces (APIs).

Principal Service Commitments and System Requirements

Management's Description of the TSG Platform was prepared to describe the procedures and controls the Company implemented to manage the risks that threaten the achievement of the service organization's service commitments and system requirements. The disclosure of the principal service commitments and system requirements enables report users to understand the critical objectives that drive the system's operation.

Service Commitments

Service commitments include those made to user entities and others (such as customers of user entities) to the extent those commitments relate to the trust services category or categories addressed by the description. Security objectives and commitments are made available to customers through managed service agreements, and other details are made available on the public-facing website. The following summarizes the Company's principal service commitments that management believes to be relevant to the report users:

- The Company uses commercially reasonable physical, managerial, and technical safeguards designed to secure data from accidental loss and unauthorized access.
- Sensitive customer messaging data is encrypted at rest.
- Content is transferred over end-to-end encryption using TLS at every point of transfer.
- Multi-factor authentication is mandatory for access to sensitive resources and is implemented for other systems when possible.
- The Company continuously monitors access to its infrastructure.

System Requirements

The Company's system requirements are communicated in system policies and procedures, system design documentation, and customer agreements. Information security policies define an organization-wide approach to protecting systems and data and include descriptions and expectations for the system's design, development, and operation. In addition to these policies, standard operating procedures have been prepared to describe specific manual and automated processes required to operate and develop services provided.

Components of the System

A system is designed, implemented, and operated to achieve specific business objectives according to management-specified requirements. The boundaries of the system described in this description include the system components related to the service life cycle, such as initiation, authorization, processing, recording, and reporting for the services provided to user entities. The system boundaries do not include instances in which transaction-processing information is combined with other information for secondary purposes internal to the service organization, such as accounting and billing.

The components of the Platform can be classified into the following five categories:

Infrastructure: The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.

Software: The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications, desktop, or laptop applications.

People: The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).

Data: The types of data used by the system, such as transaction streams, files, databases, tables, and other outputs used or processed by the system.

Procedures: The automated and manual procedures related to the services provided, including procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

The Company leverages the experience and resources of Amazon Web Services (AWS) to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the Platform architecture within the cloud hosting environment to ensure security and resiliency requirements are met. The specific resources leveraged from AWS include the following:

Cloud Hosting Services	
Service	**Description**
AWS Elastic Compute Cloud	Compute service
Amazon ECR	Managed container registry
Amazon Aurora	Managed relational database management system
RabbitMQ	Message queue manager
AWS Elastic Load Balancer	Distributes network traffic across available resources
Amazon CloudWatch	Infrastructure resource and application monitoring
AWS CloudTrail	Communication hub
Amazon GuardDuty	Threat detection service
Amazon Route 53	Domain Name System
AWS S3	Object storage
Amazon Inspector	Security assessment and vulnerability management service
AWS WAF	Managed web application firewall service
AWS Direct Connect	Allows the Platform to bypass the public internet and connect directly to the Syniverse global communications network
AWS Virtual Private Cloud	Provides a logically isolated virtual network that uses network security groups to control traffic

Software

Software consists of the programs and software that support the Platform. The list of software and ancillary software used to build, support, secure, maintain, and monitor the Platform includes the following:

Software Summary	
Application	**Purpose**
Drata, Secureframe	Compliance management platform
GitHub	Source code repository
Microsoft 365	Email, file sharing, messaging, and other tools
Azure Active Directory	Identity and authentication
Asana	Project management and issue tracking
Slack	Communication hub
Grafana, Prometheus, Loki	Metrics, logging, and dashboards
Pagerduty	Alerting
Bugsnag	Error monitoring and application stability monitoring
Zendesk	Customer service and relationship management
Dropbox/Google Drive	Company file storage
1Password	Password manager
Google Analytics	Analytics and tracking data
Hubspot	Customer relationship management

Critical Tools and Resources

The Information Security Program and scope of the system description apply to all infrastructure and software identified in the previous sections. Control activities and procedures are applied to internal systems using a risk-based approach that primarily considers the sensitivity of information stored or processed by the system and its role in maintaining the security of the Company's information.
The systems deemed by management to be vital to meeting its service commitments and system requirements are defined as "Critical Tools and Resources" throughout this description. They include the following:

- AWS
- GitHub
- Azure Active Directory

People

The Company's organizational structure provides the framework for the management, operation, and security of the Platform. The table below summarizes the key roles and functional responsibilities of the Company. Due to the Company's size, one individual may serve multiple roles.

Organizational Structure	
Role	**Function**
CEO	Responsible for oversight of the development and performance of internal controls and the direction of company-wide activities delegated to executive management
CISO	Responsible for the design, development, maintenance, dissemination, and enforcement of the Information Security Program
Engineering	Responsible for the development, testing, deployment, and maintenance of the Platform and maintaining security.
Business Operations	Manages internal business needs such as human resources, customer success, and other administrative functions.
Legal	Responsible for compliance and legal function of the Company and includes external attorneys providing services under the supervision of management.

Aggregators and Carriers

The Platform connects to several industry text message (SMS/MMS) and voice aggregators, including, but not limited to, companies such as Syniverse Technologies LLC, iconectiv TruReach Deliver Aerialink, and others (Direct Connection Aggregators). The infrastructure leverages AWS Direct Connect, VPNs, and other methods to connect directly to these Aggregators and send outbound and receive inbound traffic. Wherever possible, the Platform utilizes both primary and secondary connections to available upstream data centers to provide redundancy to customers.

Once traffic is handed off to upstream Aggregators, it is the responsibility of the Aggregator to deliver traffic to the respective mobile wireless carriers, such as AT&T, T-Mobile, and Verizon (Mobile Network Operators), and wireline carriers, such as CenturyLink, Comcast, and others, (Carriers) depending on the traffic type and destination number type. It is then the responsibility of the Carriers to deliver the traffic to the targeted consumer subscribers (phone number) and their respective handsets or networks.

The Carriers, as well as resellers, must meet certain obligations set forth by the Federal Communications Commission (FCC). The Company is required to file an FCC form 499-Q quarterly to meet compliance requirements, as well as an annual FCC form 499-A. This form is used to calculate the FCC universal service contribution factor (USCF) and circularity factor, as well as to calculate the Company's monthly universal service contribution obligation. The Company is also required to adhere to the provisions contained within Telephone Consumer Protection Act (TCPA) and makes efforts to ensure customers comply with MSAs and other agreements.

The Aggregators and Carriers are not within the scope of this system description. While these companies are technically deemed vendors and are monitored as such, the options for services provided by the Company are highly limited due to the monopolistic nature of the telecom industry. The Company takes an active stance in preventing fraud in the telecommunications industry, is a member of several industry working groups, and is a registered entity in the FCC's Robocall Mitigation Database (RMD).

Procedures

Procedures are the specific actions undertaken to implement a process, consisting of linked procedures designed to accomplish a particular goal. Policies, which serve as the basis of procedures, are management's statements of what should be done to meet system objectives and may be documented, explicitly stated in communications, or implied through actions and decisions.

The Company has adopted the following defined set of information security standards and policies (described as the Information Security Program throughout the report):

- Acceptable Use Policy
- Asset Management Policy
- Backup Policy
- Business Continuity Plan
- Code of Conduct
- Data Classification Policy
- Data Deletion Policy
- Data Protection Policy
- Disaster Recovery Plan
- Encryption Policy
- Incident Response Plan
- Information Security Policy
- Password Policy
- Responsible Disclosure Policy
- Risk Assessment Policy
- Software Development Lifecycle Policy
- System Access Control Policy
- Vendor Management Policy
- Vulnerability Management Policy

Data

Data refers to the transaction streams, files, data stores, tables, and output used or processed by the Company. Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established with customers and business partners. The following table details the types of data collected by the Company in connection with the Platform's services and the infrastructure, software, and third-party vendors utilized to store and process the data.

Data Type Summary		
Type	**Description**	**Storage and Processing**
Account data	Personally Identifiable Information and other data from personnel and other third parties such as suppliers, vendors, and business partners	AWS and certain 3rd party SaaS tools described in the Software Summary
User data	Contact information, message history, and other data related to telecommunication services	AWS
Log information	Information relevant to and explicitly necessary for services, including metadata	Grafana, AWS CloudTrail, Amazon CloudWatch
Analytics data	Product usage and tracking data are sent to analytics services to analyze usage patterns and inform product decisions	AWS, HubSpot, Google Analytics

System Incidents

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements for the period April 3, 2022 to April 2, 2023.

Applicable Trust Services Criteria and Related Controls

The trust services criteria are classified into five categories: security, availability, processing integrity, confidentiality, and privacy. Depending on which category or categories are included within the scope of the description, the applicable trust services criteria consist of criteria common to all five of the trust services criteria (common criteria) and additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories. The common criteria constitute the complete set of criteria for the security category.

The trust services categories in scope for this report are as follows:

Security: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the confidentiality of information or systems and affect the entity's ability to meet its objectives.

The common criteria are organized as follows:

Control Environment: Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

Communication and Information: Systems, both automated and manual, that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.

Risk Assessment: The entity's identification and analysis of relevant risks to achieving its objectives, forming a basis for determining how the risks can be managed.

Monitoring Activities: The criteria relevant to how the entity monitors the system, including the suitability of the design and operating effectiveness of controls, and acts to address deficiencies identified.

Control Activities: The policies and procedures that help make sure that management's directives are carried out.

Logical and Physical Access Controls: The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.

System Operations: The criteria relevant to how the entity manages the operation of systems and detects and mitigates processing deviations, including logical and physical security deviations.

Change Management: The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.

Risk Mitigation: The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Control Environment

The Company's control environment describes a set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. A control environment is the foundation on which an effective system of internal control is built and operated in an organization that strives to achieve its strategic objectives, provide reliable reporting to internal and external stakeholders, operate its business efficiently and effectively, comply with all applicable laws and regulations, and safeguard its assets.

Integrity and Ethical Values

Integrity and ethical behavior are the products of the Company's ethical and behavioral standards, communicated, monitored, and enforced in its business activities. The Company has established standards of conduct that outline its commitments to integrity and ethical values. These commitments include management's actions to remove or reduce incentives, pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. The standards of conduct are made available to all personnel, and each individual is required to acknowledge their review and understanding of its requirements upon hire and annually thereafter.

Oversight Responsibility

The Company has determined an independent board of directors is not necessary at this time. The size and complexity of the organization allow the CEO to provide personal oversight over organizational structure operations, the ability to affect ethical values, and the ability to attract, retain and hold personnel accountable. The CEO and CISO actively participate in the operation of key controls (by exercising a high level of supervision and review) to provide adequate oversight of internal control and mitigate risks. The CEO and CISO generally meet weekly for one-on-one meetings, held at a minimum each quarter, to evaluate the fulfillment of Company objectives, changes in the environment, and operational effectiveness of system controls. The Company holds a weekly technical meeting to discuss open tickets and review a standing agenda that includes strategic issues and challenges applying the Scrum Framework.

Organizational Structure, Authority, and Responsibility

The Company's organizational structure provides the framework within which its activities for achieving objectives are planned, executed, and monitored. A formal organizational chart is in place to communicate key areas of authority, responsibility, and applicable reporting lines to personnel. Management established the operating structure based on its size and the nature of its control environment and designed reporting lines to establish key areas of authority and the proper flow of information. Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Program. Job requirements and responsibilities are documented and communicated in formal job descriptions for new positions.

Commitment to Competence

Management demonstrates its commitment to competence through established policies and practices that attract, develop, and retain sufficient and competent individuals to support the achievement of objectives. The Company has implemented a security training program that must be completed for all personnel upon hire and renewed annually. The primary objective of the security training program is to educate personnel on their responsibility to protect the confidentiality, availability, and integrity of the Company's information.

Management has established formal and informal procedures that consider the background and technical competency of potential and existing personnel and vendors when determining whether to hire or retain the individual. Background verification checks on personnel are performed prior to onboarding in accordance with relevant laws and regulations and proportional to business requirements and perceived risks.

Accountability

The Company expects individuals to be held accountable for their internal control responsibilities in pursuing objectives. Management establishes performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct and considering the achievement of both short-term and long-term objectives. Individual performance is evaluated annually through a documented, formal performance review process. External contractors and other 3rd parties are engaged via written contracts that are reviewed periodically, at least annually, and would not be renewed if performance problems are experienced.

External Individuals

The Company's commitment to integrity and ethical values extends to its use of contractors and vendors. Management considers the use of service providers, who may impact security, confidentiality, and privacy in its processes to establish conduct standards, evaluate adherence to those standards, and promptly address deviations. Information security requirements for mitigating the risks associated with a supplier's access to the Company's assets are formalized with the supplier and documented.

Service providers, such as contractors, who may impact the security of the production environment or have access to customer data, are required to read and accept a non-disclosure agreement. As a general practice, the Company leverages the services of vendors generally accepted in the industry and typically shares their commitments towards security, confidentiality, and privacy available to the public, which is reviewed by personnel to ensure consistency with the Company's policies.

Communication and Information

A critical objective for the Company is ensuring relevant, and quality information is obtained or generated to support the functioning of internal control. The Company has established processes to identify information requirements and ensure appropriate internal and external sources of information are properly captured to support the functioning of other internal control components. Network architecture diagrams have been prepared and are shared with authorized individuals to communicate information about system operation and boundaries.

Internal Communication

The Company has a defined Information Security Program that describes policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements. The Information Security Program is made available to all personnel in the Company's compliance management platform. Personnel are required to review and acknowledge the Information Security Program upon hire and re-certify their acknowledgment each year. Management also reinforces the Information Security Program in meetings, internal communication, and during annual security training and awareness programs.

Management has established specific communication channels to ensure personnel have the necessary information to understand and carry out their internal control responsibilities. Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, all-hands meetings are held frequently to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the all-hands meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. The Company considers the timing, audience, and nature of the information when selecting the appropriate communication medium, allowing management to communicate changes to control objectives in a timely manner.

The Information Security Program identifies personnel responsible for designing, developing, implementing, operating, maintaining, or monitoring system controls. Formal procedures are established and documented in the Company's policies and plans for incident response that describe how to report systems failures, incidents, concerns, and other complaints to personnel.

External Communication

The Company has prioritized maintaining open communication channels with external parties that allow input from customers, business partners, external auditors, and others to provide management with relevant information. The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations. Agreements are established with critical vendors and business partners that clearly define terms, conditions, and responsibilities. Security objectives and commitments are made available to customers through managed service agreements, and other details are made available on the public-facing website.

Product updates are shared with customers so the Company can continue to innovate and maintain the security of the Platform. Multiple marketing channels are available to share new features, and the Company selects the appropriate method, frequency, and messaging based on the specific feature being shared. The Company communicates changes that impact security or user functionality to clients through direct communication via email and the use of a support page that shares release notes and network maintenance windows. Significant changes, such as those that require action by the user to maintain functionality or impact security requirements, are communicated to users directly and in advance of the implementation.

The Company makes available information about the design and operation of the Platform and its boundaries to clients through an online knowledgebase made available within the application. Customers and other external users are provided with information on reporting systems failures, incidents, concerns, and other complaints to appropriate personnel.

Risk Assessment

The Company has a defined risk management program to provide guidance applied to identify potential threats, rate the significance of the risks associated with the threats, and apply mitigation strategies for those risks. The first step of the risk assessment process is to identify assets within the scope of the Information Security Program. The objectives identified by management are specified in the risk management program to identify and assess risk related to the objectives.

The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to assets and service commitments are identified, and the risks are formally assessed. The risk assessment includes considering the potential for fraud and how fraud may impact the achievement of objectives. The Company's fraud risk assessment considers incentives, opportunities, and attitudes of management and other personnel to override controls and result in fraud or general misconduct and the specific fraud risks that arise from information technology and access to information.

Risk management discussions include a consideration of how changes in the environment impact risk, such as revisions to the Company's business model, personnel turnover, and the implementation of new systems and technology, which may create new risks that could significantly impact the Company's ability to meet its objectives. The Engineering Team meets on an ad hoc basis to prioritize and monitor mitigation strategies so the team can react to emerging risks.

Monitoring Activities

The Company selects, develops, and performs ongoing and, if necessary, separate evaluations to ascertain whether the components of internal control are present and functioning. Management considers the rate of change in business and business processes when selecting and developing separate ongoing evaluations and utilizes the current state of the internal controls to establish a baseline. The following describes the primary methods currently utilized by management:

Penetration Testing: The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution. The penetration tests are performed by a certified penetration tester to identify specific technical threats and vulnerabilities and to benchmark the environment against leading cybersecurity practices.

Vulnerability Scanning: The Company utilizes Amazon Inspector to continuously scan the environment for software vulnerabilities and unintended network exposure. Alerts are provided to management upon the identification of a vulnerability and are prioritized and remediated according to risk.

Monitoring of Cloud Environment: The Company evaluates risks related to cloud hosting providers and reviews current SOC 2 Type 2 reports or other procedures as deemed necessary. Management continually evaluates the cloud hosting providers' shared responsibility model to ensure required shared controls and customer-specific controls are in place and uses tools to monitor the environment. Logs are aggregated centrally and monitored for indicators of compromise. Alerts are generated based on thresholds established to define potential suspicious activity and reviewed by the appropriate personnel. Production systems are configured to monitor, log, and self-repair or alert on suspicious changes to critical system files and unauthorized intrusions and access attempts.

The results of ongoing and separate evaluations are provided to the appropriate individuals to assess results. The Company uses internal tools to aggregate and monitor identified deficiencies, alert the individuals responsible for corrective action, and provide visibility to senior leaders regarding the timeliness of remediation.

Control Activities

Control activities are the actions established through policies and procedures that help ensure management's directives to mitigate risks to achieve objectives are carried out. They may be preventative or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews.

Compliance Management Platform

Management leverages a compliance management platform to support the design, implementation, operation, monitoring, and documentation of its control activities. The platform captures data via APIs across multiple technology providers, including identity providers, infrastructure providers, version control systems, ticketing systems, and human resource information systems, to provide a central dashboard for compliance activities. The compliance management platform is also utilized to support the following:

- Continuous automated monitoring of certain security controls
- Compliance checks on personnel workstations
- Inventory management
- Communication and documentation of review, approval, and acknowledgment of information security policies
- Real-time visibility to manage the Information Security Program

Use of a compliance management platform does not relieve management of its responsibilities for designing, implementing, and operating the Information Security Program. Management is also responsible for evaluating the accuracy and completeness of the information produced, maintained, and aggregated by the compliance management platform, which is performed through an annual risk assessment and necessary due diligence procedures, such as obtaining and reviewing the platform's most recent SOC 2 Type 2 report; which includes the trust services criteria related to processing integrity.

Information Security Program Development and Maintenance

As part of its annual risk assessment, management selects and develops control activities that mitigate risks to acceptable levels and contribute towards the achievement of organizational objectives. The risk assessment process includes the selection and development of control activities over technology infrastructure, designed and implemented to help ensure the completeness, accuracy, and availability of technology processing. Specifically, management selects and develops control activities designed and implemented to restrict technology access rights and achieve management's objectives over the acquisition, development, and maintenance of technology and infrastructure.

The Information Security Program is reviewed by management annually and approved by the CISO. The Company's policies and procedures are designed to govern an individual's day-to-day activities and establish expectations and relevant procedures specifying actions. Management assigns competent personnel with sufficient authority the responsibility to promptly perform control activities and duties with diligence and continuing focus.

Logical and Physical Access Controls

The Company has established policies and procedures that define the access control requirements for requesting and provisioning user access to the system. Duties and access to sensitive resources are established based on the principle of least privilege. Logical access to systems is restricted through access control software and rule sets and is controlled by limited administrative users. Individuals require a unique username and are identified and authenticated before accessing information assets. Access to Critical Tools and Resources requires multi-factor authentication.

The Company has established a formal onboarding and termination process. Appropriate management approval is obtained before granting access to Critical Tools and Resources. The Company's compliance management platform performs automated checks and triggers alerts if users access certain resources without appropriate approval and completion of the onboarding process. System access reviews are performed annually. Accounts for personnel who have been terminated or no longer require access are disabled within one business day.

Privileged access to Critical Tools and Resources is highly restricted. Users with multiple access levels (e.g., administrators) are given separate accounts for normal system use and administrative functions. The Company's production systems can only be accessed by authorized personnel via an approved encrypted connection (e.g., OpenVPN, SSH, and IP whitelisting associated with AWS Security Groups). Access to migrate changes to production is restricted to authorized individuals with a business need.

Full-disk encryption is implemented for all personnel workstations and laptops. Personnel accessing Critical Tools and Resources utilize laptops with the most recent operating system security updates and configured with antivirus software.

Management maintains a detailed inventory of all information systems, including classification and prioritization based on the asset's business value and criticality to the Company. Information and data assets are subject to the Company's policies and procedures for data protection, classification, and retention, which define parameters for the ownership, classification, security, storage, and retention of data. Formal data retention and disposal procedures are in place to guide the secure retention and disposal of Company and customer data.

The Company's policies and procedures define the requirements for proper and effective use of cryptography to protect information confidentiality, authenticity, and integrity. Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks. Specifically, information transmitted to Syniverse is performed utilizing a private network connection provided by AWS Direct Connect. Encryption is used to protect sensitive messaging data at rest, which is a managed service provided by AWS. Customer data is encrypted when stored in database tables, temporary files, and backups using 256-bit Advanced Encryption Standard.

Points of access by outside entities and the types of data that flow through the access points are identified, inventoried, and managed. The Company uses firewalls and configures them to protect against threats from sources outside the system's boundaries. Management reviews its firewall rules at least annually, and required changes are tracked to completion. A threat detection service is implemented to monitor and detect unauthorized access attempts.

Infrastructure supporting the service is monitored for malware by the Company and AWS through a shared responsibility model. Infrastructure resources consist of containerized applications, managed by Kubernetes and built from hardened Docker images, that are subject to vulnerability scanning. The Company uses a private Amazon Elastic Container Registry (Amazon ECR) that provides API operations to create, monitor, and delete image repositories and set permissions. The Company's continuous delivery/deployment (CD) pipeline checks for signed images, and signed images are part of the continuous integration (CI) process by which the Engineering Team sign commits to the Company's private GitHub repository.

System Operations

The Company has established baseline configuration standards for production servers and uses tools to detect and restore server configuration deviations from the standards. Infrastructure is monitored for noncompliance with the configuration standards, which could threaten the achievement of the Company's objectives. Certain third-party tools and procedures are used to identify potential vulnerabilities and deficiencies. Identified security deficiencies are tracked and prioritized through internal tools according to their severity.

Applicable security patches are applied immediately or during a scheduled release to the environment based on the severity of the vulnerability. Processes are in place to evaluate patches and their applicability to the environment. Once the patches have been reviewed, and their criticality level is determined, service teams determine the patch implementation strategy.

Formal procedures are defined for security event detection and management, including the provision of resources. The Company uses a system that collects and stores server logs in a central location. The system can be queried in an ad hoc fashion by authorized users. Activity logs and other data sources are analyzed by continuous monitoring tools to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Personnel are assigned to configure the monitoring tools, and the appropriate individuals receive real-time alerts through the generation of emails and alarms.

The Company has established plans for incident response that outline management responsibilities and procedures to respond to information security incidents. Security events are quantified, monitored, and tracked by an identified incident response team, and procedures specified include collecting and preserving information that can serve as evidence. Appropriate communication channels have been established to share the necessary information regarding security events with management, users, and other key individuals. Post-mortem meetings are conducted for security incidents to discuss the root causes, remediation steps, and lessons learned. The Company's plans for incident response require creating, prioritizing, assigning, and tracking follow-ups to completion.

Change Management

The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems. The change management processes and procedures have been established to plan, schedule, apply, distribute, and track changes to the production environment to minimize risk and client impact.

The Company uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Software developers are expected to adhere to the Company's coding standards throughout the development cycle, including standards for quality, commenting, and security. Releases are tested before deployment, and a release checklist must be completed before deploying code, which includes a checklist of all associated tests. Production and development systems are maintained separately using separate servers and databases.

The Company's engineers perform development utilizing an agile framework and continuously release iterative changes in a collaborative environment. Primary development activities are implemented by two highly experienced engineers, and code reviews are performed for significant pull requests prior to releasing them to production. A separate review may not be deemed practical for all changes, but any change in the production environment is automatically communicated to the Engineering Team, including the CISO, through an integration with Slack. Overrides of edit checks, approvals, and changes to confirmed transactions are appropriately authorized, documented, and reviewed, and access to migrate changes to production is restricted to authorized personnel with a business need. The Company communicates changes to customers through direct email and/or the use of a support page (support.tsgglobal.com) that shares release notes and network maintenance windows.

Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the Company's commitments and system requirements. Upon the identification of a deficiency, processes are in place for authorizing, designing, testing, approving, and implementing changes necessary in the event a change needs to be implemented in an urgent timeframe.

Risk Mitigation

The Company implements risk mitigation strategies to prioritize, evaluate, and implement the appropriate risk-reducing controls recommended by the risk management process. Management has identified potential business disruptions as a critical risk to meeting its objectives and has established plans for business continuity, disaster recovery, and incident response to respond to, mitigate, and recover from security events that could disrupt business operations. These plans are documented and made available to Company personnel to provide guidance for detecting, responding to, and recovering from security events and incidents. The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes consideration of risks arising from potential business disruptions and the identification of mitigation strategies.

As part of its risk mitigation strategies, management assesses and manages risks associated with vendors and business partners. Periodically, generally annually, but performed relative to risk and changes in the environment, management assesses the risks that vendors and business partners represent to the achievement of the Company's objectives. As a general practice, the Company utilizes software and infrastructure resources and applications that are industry leaders and generally accepted amongst the security community.

The vendor management process includes maintaining an inventory of third-party vendors, categorization of vendor risks based on access levels, criticality to services provided, and other factors, and a review of the vendor's security and privacy requirements. Based on the risk assessment, management obtains due diligence and compliance information, such as SOC 2 Type 2 reports, requested and reviewed during the vendor acceptance and re-review process. The Company has written agreements in place with vendors and business partners that include confidentiality and privacy commitments consistent with the commitments and requirements of the Company.

User Entity Controls and Responsibilities

The Company's services are designed utilizing a shared responsibility model where maintaining the security of a customer's information is dependent upon the customer implementing controls that are outside the Company's control. If these controls are necessary to meet the Company's service commitments and system requirements, they are known as complementary user entity controls (CUECs) as defined by DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report*. Other controls that are necessary or recommended for the customer to maintain the security of its information are defined as user entity responsibilities.

Complementary User Entity Controls

The Company has restricted its service commitments to matters for which it is responsible, and that can be reasonably achieved by itself, and the Platform's system requirements are derived from those commitments. Therefore, CUECs are not required or significant to achieve the service commitments and system requirements based on the applicable trust services criteria.

User Entity Responsibilities

The Company communicates the expectations or requirements of its users through legal agreements and instructional material, such as user manuals, which are necessary to allow the customer to benefit from the use of the Platform. User entity responsibilities are generally either explicitly required or communicated as a recommended best practice, and the controls presented below should not be regarded as a comprehensive list of controls that user entities should implement.

User entity responsibilities that should be implemented to allow the customer to benefit from the use of the Platform include the following:

- Ensuring the confidentiality of user accounts and passwords
- Notifying the Company promptly when changes are made to technical, billing, or administrative contact information
- Developing internal disaster recovery and business continuity plans that address the inability to access or utilize the Company's services
- Notifying the Company and providing accurate information regarding new, terminated, and changes necessary to user accounts
- Informing the Company of any regulatory issues that may affect the services provided
- Understanding and complying with contractual obligations to the Company
- Immediately notifying the Company of any actual or suspected information security breaches involving the Platform, including compromised user accounts
- Granting access only to authorized and trained personnel
- Deploying physical security and environmental controls for all devices and access points

Subservice Organization Controls

When controls at a vendor are necessary in combination with the Company's controls to provide reasonable assurance that the Company's service commitments and system requirements are achieved, based on the applicable trust services criteria, the vendor is considered a subservice organization. Complementary subservice organization controls (CSOCs) are controls that the Company's management assumed, in the design of the system, would be implemented by subservice organizations and are necessary, in combination with controls at the Company, to provide reasonable assurance that the Company's service commitments and system requirements were achieved. Management has identified the below subservice organization and has elected to use the carve-out method for the purposes of this report:

Complementary Subservice Organization	
Subservice Organization	**Description**
AWS	Cloud hosting services

The Company is responsible for the oversight and monitoring of its subservice organization, which is subject to vendor management policies and procedures. Management regularly reviews technical resources made available through the cloud provider's website, technical training, and industry forums to understand key concepts and implement controls necessary to meet the Company's responsibilities described in the shared responsibility model for each specific service utilized. Management also reviews the cloud provider's SOC 2 Type 2 report annually and monitors the subservice organization through regular communication and interaction with the environment.

The following are the applicable trust services criteria and controls that are necessary to be in place at the subservice organization to provide reasonable assurance that the Company's service commitments and system requirements were achieved:

Complementary Subservice Organization Controls	
Criteria	**Control**
Logical and Physical Access CC6 Series	Procedures are implemented to authenticate authorized users, restrict physical and logical access, and detect unauthorized access attempts and procedures are implemented to decommission and physically destroy production assets securely. Security measures are implemented to provision and deprovision user access to systems and applications based on appropriate authorization, and encryption has been implemented, by default or as configured by the Company, to secure the transmission and storage of information.

Complementary Subservice Organization Controls	
Criteria	**Control**
System Operations CC7 Series	Vulnerability scans and penetration testing are performed periodically to identify system vulnerabilities, and environmental protection, monitoring, and procedures for regular maintenance are implemented at the data center facilities. Incident response procedures are established and implemented to identify, analyze, and remediate events and incidents.
Change Management CC8 Series	Procedures are established and implemented to ensure system changes are authorized, designed, developed, configured, documented, tested, and approved before production deployment.

Trust Services Criteria Relevance

All security trust services criteria as set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* were relevant to the Platform as presented in this report.

Significant Changes to the Platform

There have been no changes that are likely to affect report users' understanding of how the Platform is used to provide services for the period April 3, 2022, to April 2, 2023.

Use of Report

The description does not omit or distort information relevant to the Platform while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each user may consider important to their own particular needs.

Section 4

Information Provided by Service Auditor

Information Provided by Service Auditor

Engagement Objectives and Scope

A SOC 2 report is intended to provide users of the TSG Platform with the information necessary to help assess and address the risks associated with the services provided by the Platform. The report is intended for use by those with sufficient knowledge and understanding of the Platform, its services, and the system used to provide those services, among other matters. Without such knowledge, users are likely to misunderstand the contents of the SOC 2 report. Thus the Independent Service Auditor's Report of MJD Advisors, LLC (MJD) provided in Section 1 is restricted to specified parties who possess the requisite knowledge.

MJD's responsibility in this report is to perform a SOC 2 examination in accordance with AT-C Section 105, *Concepts Common to All Attestation Engagements*, and AT-C Section 205, *Examination Engagements*. According to those standards, the examination is predicated on the concept that management is responsible for the design, implementation, and operating effectiveness of its controls to provide reasonable assurance the organization's service commitments and system requirements were achieved. Management is also responsible for preparing the System Description in Section 3 and Management's Assertion in Section 2 of this report, including the completeness, accuracy, and method of presentation. MJD's responsibility is to design and perform procedures to obtain sufficient appropriate evidence and express an opinion on the presentation of the description and the design and operating effectiveness of controls.

Management of TSG Global, Inc is responsible for determining the point in time (SOC 2 Type 1) or period of time (SOC 2 Type 2) to be covered by the description of the Platform, its assertion, and, consequently, the service auditor's examination. The frequency and period covered by a SOC 2 report is a business decision of management, determined by the needs of its users, and management determined that a SOC 2 Type 2 report was appropriate in the circumstances. MJD's responsibility is to express an opinion on the description and the suitability of the design and operating effectiveness of controls, further described in Section 1.

Control Matrix for the TSG Platform

The control matrix that follows is to provide report users with the specific controls management has identified to meet the applicable trust services criteria. MJD's tests of the operating effectiveness of those controls included such tests considered necessary in the circumstances to evaluate whether those controls were sufficient to provide reasonable, but not absolute, assurance the Company's service commitments and system requirements were achieved based on the applicable trust services criteria relevant to security throughout the period April 3, 2022, to April 2, 2023.

Tests of controls included inquiry of appropriate management, supervisory and staff personnel, observation of the Company's activities and operations, and inspection of documents and records. In selecting particular tests of the operating effectiveness of the controls, we considered multiple factors, such as (*a*) the characteristics of the population of the controls to be tested, including the nature of the controls; (*b*) whether the population is made up of homogenous items; (*c*) the frequency of the controls' application; and (*d*) the expected deviation rate. Where appropriate, we utilized a sample-based testing strategy in accordance with the AICPA Audit Guide, *Audit Sampling*, developed by the AICPA *Audit Sampling* Guide Task Force. As inquiries were performed for substantially all the Company's controls, this test was not listed individually for every control in the control matrix below.

For tests of controls requiring the use of information produced by the entity (IPE), MJD performed one or more of the following procedures to address the completeness, accuracy, and data integrity of the data or reports provided:

- Inspected the source of the data or report
- Inspected the query, script, or parameters used to generate the data or report
- Observed the generation of the data or report
- Agreed data between the report and the source

In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of controls (e.g., periodic reviews of user access listings), MJD evaluated management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or report.

Control Environment

CC1.1: The entity demonstrates a commitment to integrity and ethical values.		
Control Description	**Tests Performed by MJD**	**Results**
The Company's standards of conduct outline its commitments to integrity and ethical values.	Inspected the Company's standards of conduct to determine they outlined a commitment to integrity and ethical values.	No deviations noted.
The standards of conduct are made available to all personnel, and each individual is required to acknowledge their review and understanding of its requirements upon hire and annually thereafter.	Observed evidence the Company makes the standards of conduct available to all personnel. Inspected signed acknowledgments of the standards of conduct for a selection of current personnel to ascertain each was completed annually. Inspected signed acknowledgments of the Company's standards of conduct for a selection of new personnel to ascertain it was completed during the onboarding process.	No deviations noted.
Background verification checks on personnel are performed prior to onboarding in accordance with relevant laws and regulations and proportional to business requirements and perceived risks.	Inspected the Information Security Program to ascertain the requirements for background verification checks to be performed on personnel before onboarding in accordance with relevant laws and regulations and proportional to business requirements and perceived risks. Inspected background verification checks for a selection of new personnel to ascertain background screening procedures were performed based on the perceived risk of the position.	No deviations noted.
Vendors and business partners are subject to due diligence procedures that include a review of security, confidentiality, and privacy commitments provided through terms of service and written agreements to ensure consistency with the commitments and requirements of the Company.	Inspected evidence of the due diligence procedures performed for a selection of critical vendors to ascertain management reviewed the terms of service, privacy policy, and other information provided by the vendor, as needed, to determine the security, confidentiality, and privacy commitments were consistent with the requirements established by the Company.	No deviations noted.

Control Environment

CC1.2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
Control Description	**Tests Performed by MJD**	**Results**
The CEO and CISO actively participate in the operation of key controls (by exercising a high level of supervision and review) to provide adequate internal control oversight and mitigate risks.	Inspected the Information Security Program and discussed the procedures with the CISO to ascertain the CEO and CISO's responsibilities include the supervision and review of key controls.	No deviations noted.
The CEO and CISO hold regular meetings to evaluate the fulfillment of Company objectives, changes in the environment, and operational effectiveness of system controls.	Observed the recurring calendar reminder for the CEO and CISO and reviewed the executive issue tracker board to ascertain regular meetings are held, and systems are established to track executive priorities.	No deviations noted.

CC1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
Control Description	**Tests Performed by MJD**	**Results**
A formal organizational chart is in place to communicate key areas of authority, responsibility, and applicable lines of reporting to personnel.	Inspected the organizational chart to ascertain it defined areas of authority, responsibility, and reporting lines.	No deviations noted.
Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Program.	Inspected the Information Security Program to ascertain it formally assigned the responsibility for the design, development, implementation, operation, maintenance, and monitoring of information security controls.	No deviations noted.
Job requirements and responsibilities are documented and communicated in formal job descriptions for new positions.	Inspected the Company's online job postings and the job description template to ascertain the requirements and responsibilities for new positions are documented and communicated for new positions.	No deviations noted.

Control Environment

CC1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
Control Description	**Tests Performed by MJD**	**Results**
The standards of conduct are made available to all personnel, and each individual is required to acknowledge their review and understanding of its requirements upon hire and annually thereafter.	Observed evidence the Company makes the standards of conduct available to all personnel. Inspected signed acknowledgments of the standards of conduct for a selection of current personnel to ascertain each was completed annually. Inspected signed acknowledgments of the Company's standards of conduct for a selection of new personnel to ascertain it was completed during the onboarding process.	No deviations noted.
Job requirements and responsibilities are documented and communicated in formal job descriptions for new positions.	Inspected the Company's online job postings and the job description template to ascertain the requirements and responsibilities for new positions are documented and communicated for new positions.	No deviations noted.
The Company has implemented a security training program that is required to be completed for all personnel upon hire and renewed each year.	Inspected evidence of the completion of the security training program for a selection of current personnel to ascertain it was completed annually. Inspected evidence of the completion of the security training program for a selection of new personnel to ascertain it was completed during the onboarding process.	No deviations noted.
Background verification checks on personnel are performed prior to onboarding in accordance with relevant laws and regulations and proportional to business requirements and perceived risks.	Inspected the Information Security Program to ascertain the requirements for background verification checks to be performed on personnel before onboarding in accordance with relevant laws and regulations and proportional to business requirements and perceived risks. Inspected background verification checks for a selection of new personnel to ascertain background screening procedures were performed based on the perceived risk of the position.	No deviations noted.

CC1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
Control Description	**Tests Performed by MJD**	**Results**
Individual performance is evaluated annually through a documented, formal performance review process.	Selected current personnel and reviewed the performance reviewed documentation to ascertain a performance review had been performed during the scope period.	No deviations noted.

Control Environment

CC1.5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
Control Description	**Tests Performed by MJD**	**Results**
The Company's standards of conduct outline its commitments to integrity and ethical values.	Inspected the Company's standards of conduct to determine they outlined a commitment to integrity and ethical values.	No deviations noted.
The standards of conduct are made available to all personnel, and each individual is required to acknowledge their review and understanding of its requirements upon hire and annually thereafter.	Observed evidence the Company makes the standards of conduct available to all personnel. Inspected signed acknowledgments of the standards of conduct for a selection of current personnel to ascertain each was completed annually. Inspected signed acknowledgments of the Company's standards of conduct for a selection of new personnel to ascertain it was completed during the onboarding process.	No deviations noted.
Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Program.	Inspected the Information Security Program to ascertain it formally assigned the responsibility for the design, development, implementation, operation, maintenance, and monitoring of information security controls.	No deviations noted.
Individual performance is evaluated annually through a documented, formal performance review process.	Selected current personnel and reviewed the performance reviewed documentation to ascertain a performance review had been performed during the scope period.	No deviations noted.

Communication and Information

CC2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
Control Description	**Tests Performed by MJD**	**Results**
Network architecture diagrams have been prepared and are shared with authorized individuals to communicate information about system operation and boundaries.	Inspected the architecture diagram to determine it documented system boundaries and observed evidence it was made available to personnel in the compliance management platform.	No deviations noted.
The Company has a defined Information Security Program that describes policies and procedures to guide personnel in the achievement of the Company's security commitments and associated system requirements.	Inspected the Information Security Program documents to verify the Company has defined policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements. Observed evidence the Company provides the Information Security Program to all personnel through the compliance management platform.	No deviations noted.
Management maintains a detailed inventory of all information systems that includes classification and prioritization based on the asset's business value and criticality to the Company.	Inspected the inventory detail to ascertain the Company maintains a detailed inventory of physical and virtual assets.	No deviations noted.

Communication and Information

CC2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
Control Description	**Tests Performed by MJD**	**Results**
The standards of conduct are made available to all personnel, and each individual is required to acknowledge their review and understanding of its requirements upon hire and annually thereafter.	Observed evidence the Company makes its standards of conduct available to all personnel. Inspected signed acknowledgments of the standards of conduct for a selection of current personnel to ascertain each was completed annually. Inspected signed acknowledgments of the Company's standards of conduct for a selection of new personnel to ascertain it was completed during the onboarding process.	No deviations noted.
The Company has implemented a security training program that is required to be completed for all personnel upon hire and renewed each year.	Inspected evidence of the completion of the security training program for a selection of current personnel to ascertain it was completed annually. Inspected evidence of the completion of the security training program for a selection of new personnel to ascertain it was completed during the onboarding process.	No deviations noted.
Network architecture diagrams have been prepared and are shared with authorized individuals to communicate information about system operation and boundaries.	Inspected the architecture diagram to determine it documented system boundaries and observed evidence it was made available to personnel in the compliance management platform.	No deviations noted.
The Company has a defined Information Security Program that describes policies and procedures to guide personnel in the achievement of the Company’s security commitments and associated system requirements.	Inspected the Information Security Program documents to verify the Company has defined policies and procedures to guide personnel in achieving the Company’s security commitments and associated system requirements. Observed evidence the Company provides the Information Security Program to all personnel through the compliance management platform.	No deviations noted.

CC2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
Control Description	**Tests Performed by MJD**	**Results**
The Information Security Program is made available to all personnel in the Company's compliance management platform. Personnel are required to review and acknowledge the Information Security Program upon hire and re-certify their acknowledgment each year.	Observed evidence the Company provides the Information Security Program to all personnel through the compliance management platform. Inspected signed acknowledgments of the Information Security Program for a selection of current personnel to ascertain it was completed annually. Inspected signed acknowledgments of the Information Security Program for a selection of new personnel to ascertain it was completed during the onboarding process.	No deviations noted.
The Information Security Program identifies personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring system controls.	Inspected the Information Security Program to ascertain it formally assigned the design, development, implementation, operation, maintenance, and monitoring of system controls.	No deviations noted.
Formal procedures are established and documented in the Company's plans for incident response that describes how to report systems failures, incidents, concerns, and other complaints to personnel.	Inspected the procedures and plans for incident response to ascertain the policies and procedures provide guidance for reporting security failures, incidents, concerns, and other complaints to appropriate personnel.	No deviations noted.

Communication and Information

CC2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control.		
Control Description	**Tests Performed by MJD**	**Results**
Security objectives and commitments are made available to customers through managed service agreements, and other details are made available on the public-facing website.	Inspected the managed service agreement template and reviewed the Platform's website to ascertain the Company communicates its security objectives and commitments to customers.	No deviations noted.
The Company makes available information about the design and operation of the Platform and its boundaries to clients through an online knowledgebase made available within the application.	Inspected details made available within the application to ascertain information is made available to users to understand the design and operation of the Platform and its boundaries.	No deviations noted.
Customers and other external users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the Company's website to ascertain it provided contact information for reporting systems failures, incidents, concerns, and other complaints to appropriate personnel.	No deviations noted.
The Company communicates changes that impact security or user functionality to clients through direct communication via email and the use of a support page that shares release notes and network maintenance windows.	Observed the Company's support page and inspected example communications sent to users to announce product changes to ascertain the Company has channels in place to communicate product releases, bug fixes, and enhancements.	No deviations noted.
Vendors and business partners are subject to due diligence procedures that include a review of security, confidentiality, and privacy commitments provided through the terms of service and written agreements to ensure consistency with the commitments and requirements of the Company.	Inspected evidence of the due diligence procedures performed for a selection of critical vendors to ascertain management reviewed the terms of service, privacy policy, and other information provided by the vendor, as needed, to determine the security, confidentiality, and privacy commitments were consistent with the requirements established by the Company.	No deviations noted.

Risk Assessment

CC3.1: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
Control Description	**Tests Performed by MJD**	**Results**
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.	Inspected the policies and procedures pertaining to risk management to ascertain the Company has a defined, formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats.	No deviations noted.
The objectives identified by management are specified in the risk management program to enable the identification and assessment of risk related to the objectives.	Inspected the annual risk assessment and discussed the process with management to determine that the Company specified its objectives to enable the identification and assessment of risks related to objectives.	No deviations noted.
The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk management program to ascertain the requirement for risk assessments to be performed at least annually, and as part of this process, threats, fraud risks, and changes to objectives and service commitments are identified. Inspected the risk assessment to ascertain it was completed annually and was performed and documented consistently with the risk management program.	No deviations noted.

Risk Assessment

CC3.2: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
Control Description	**Tests Performed by MJD**	**Results**
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.	Inspected the risk management program to ascertain the Company has a defined, formal, risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats.	No deviations noted.
The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk management program to ascertain the requirement for risk assessments to be performed at least annually, and as part of this process, threats, fraud risks, and changes to objectives and service commitments are identified. Inspected the risk assessment to ascertain it was completed annually and was performed and documented consistently with the risk management program.	No deviations noted.
The Engineering Team meets on an ad hoc basis to prioritize and monitor mitigation strategies so the team can react to emerging risks.	Inspected evidence of Engineering Team meetings are scheduled each week and observed the team issue tracker board to ascertain the team prioritizes risk-related tasks on an ongoing basis.	No deviations noted.

Risk Assessment

CC3.3: The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
Control Description	**Tests Performed by MJD**	**Results**
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.	Inspected the risk management program to ascertain the Company has a defined, formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats.	No deviations noted.
The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk management program to ascertain the requirement for risk assessments to be performed at least annually, and as part of this process, threats, fraud risks, and changes to objectives and service commitments are identified. Inspected the risk assessment to ascertain it was completed annually and was performed and documented consistently with the risk management program.	No deviations noted.
The Company's fraud risk assessment considers incentives, opportunities, and attitudes of management and other personnel to override controls and result in fraud or general misconduct and the specific fraud risks that arise from IT and access to information.	Inspected the risk management program to ascertain the Company's fraud risk assessment is to include consideration of incentives, opportunities, and attitudes of management and other personnel to override controls and result in fraud or general misconduct and the specific fraud risks that arise from the IT and access to information.	No deviations noted.

Risk Assessment

CC3.4: The entity identifies and assesses changes that could significantly impact the system of internal control.		
Control Description	**Tests Performed by MJD**	**Results**
The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk management program to ascertain the requirement for risk assessments to be performed at least annually, and as part of this process, threats, fraud risks, and changes to objectives and service commitments are identified. Inspected the risk assessment to ascertain it was completed annually and was performed and documented consistently with the risk management program.	No deviations noted.
The Engineering Team meets on an ad hoc basis to prioritize and monitor mitigation strategies so the team can react to emerging risks.	Inspected evidence of Engineering Team meetings are scheduled each week and observed the team issue tracker board to ascertain the team prioritizes risk-related tasks on an ongoing basis.	No deviations noted.

Monitoring Activities

CC4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
Control Description	**Tests Performed by MJD**	**Results**
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company's vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the most recently completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
The Company utilizes Amazon Inspector to continuously scan the environment for software vulnerabilities and unintended network exposure. Alerts are provided to management upon the identification of a vulnerability and are prioritized and remediated according to risk.	Inspected the Amazon Inspector dashboard to ascertain continuous scanning was enabled and reviewed the status of outstanding vulnerabilities with management to determine a process was in place to evaluate and remediate the issues identified.	No deviations noted.
The Company evaluates risks related to cloud hosting providers and reviews current SOC 2 reports or other procedures as deemed necessary.	Inspected evidence of management's risk assessment and annual review of the SOC 2 report for AWS.	No deviations noted.
Logs are aggregated centrally and monitored for indicators of compromise. Alerts are generated based on thresholds established to define potential suspicious activity and are reviewed by the appropriate personnel.	Observed the monitoring dashboard for Grafana to ascertain logs are aggregated centrally and monitored for indicators of compromise. Inspected example alerts to ascertain thresholds were in place to identify potential suspicious activity, and alerts were communicated to appropriate personnel utilizing internal tools.	No deviations noted.

Monitoring Activities

CC4.2: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
Control Description	**Tests Performed by MJD**	**Results**
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company's vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the most recently completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
The Company utilizes Amazon Inspector to continuously scan the environment for software vulnerabilities and unintended network exposure. Alerts are provided to management upon the identification of a vulnerability and are prioritized and remediated according to risk.	Inspected the Amazon Inspector dashboard to ascertain continuous scanning was enabled and reviewed the status of outstanding vulnerabilities with management to determine a process was in place to evaluate and remediate the issues identified.	No deviations noted.
The Company evaluates risks related to cloud hosting providers and reviews current SOC 2 reports or other procedures as deemed necessary.	Inspected evidence of management's risk assessment and annual review of the SOC 2 report for AWS.	No deviations noted.
The Company uses internal tools to aggregate and monitor identified deficiencies, alert the individuals responsible for corrective action, and provide visibility to senior leaders regarding the timeliness of remediation.	Observed the use of any dashboards for Asana to ascertain deficiencies are aggregated centrally, assigned to the individual responsible for corrective action, and provided visibility to senior leaders regarding the timeliness of remediation.	No deviations noted.

Control Activities

CC5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
Control Description	**Tests Performed by MJD**	**Results**
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated, and mitigation strategies for those risks.	Inspected the risk management program to ascertain the Company has a defined, formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats.	No deviations noted.
As part of its annual risk assessment, management selects and develops control activities, including general control activities over technology, that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Inspected the risk management program to ascertain the risk management process is designed to be integrated with the selection or development of control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. Inspected the risk assessment to ascertain it was completed annually and was performed and documented consistently with the risk management program.	No deviations noted.
The Information Security Program is reviewed by management annually and approved by the CISO.	Inspected evidence the CISO approved the Information Security Program within the previous 12 months.	No deviations noted.
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the compliance management platform monitoring results for a selection of days to ascertain that only authorized users had access to infrastructure and the code repository. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege had been applied.	No deviations noted.

Control Activities

CC5.2: The entity also selects and develops general control activities over technology to support the achievement of objectives.		
Control Description	**Tests Performed by MJD**	**Results**
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company's vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the most recently completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
The Company utilizes Amazon Inspector to continuously scan the environment for software vulnerabilities and unintended network exposure. Alerts are provided to management upon the identification of a vulnerability and are prioritized and remediated according to risk.	Inspected the Amazon Inspector dashboard to ascertain continuous scanning was enabled and reviewed the status of outstanding vulnerabilities with management to determine a process was in place to evaluate and remediate the issues identified.	No deviations noted.
As part of its annual risk assessment, management selects and develops control activities, including general control activities over technology, that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Inspected the risk management program to ascertain the risk management process is designed to be integrated with the selection or development of control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. Inspected the risk assessment to ascertain it was completed annually and was performed and documented consistently with the risk management program.	No deviations noted.
The Information Security Program is reviewed by management annually and approved by the CISO.	Inspected evidence the CISO approved the Information Security Program within the previous 12 months.	No deviations noted.

CC5.2: The entity also selects and develops general control activities over technology to support the achievement of objectives.		
Control Description	**Tests Performed by MJD**	**Results**
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the compliance management platform monitoring results for a selection of days to ascertain that only authorized users had access to infrastructure and the code repository. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege had been applied.	No deviations noted.
System access reviews are performed annually.	Inspected the Company's policies for system access control to ascertain the requirement to perform annual reviews of user access rights. Inspected documentation of the annual system access review, performed during the scope period, and reviewed evidence any findings had been remediated timely, as deemed necessary.	No deviations noted.

Control Activities

CC5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
Control Description	**Tests Performed by MJD**	**Results**
The Company has a defined Information Security Program that describes policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements.	Inspected the Information Security Program documents to verify the Company has defined policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements. Observed evidence the Company provides the Information Security Program to all personnel through the compliance management platform.	No deviations noted.
The Information Security Program identifies personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring system controls.	Inspected the Information Security Program to ascertain it formally assigned the design, development, implementation, operation, maintenance, and monitoring of system controls.	No deviations noted.
Security objectives and commitments are made available to customers through managed service agreements, and other details are made available on the public-facing website.	Inspected the managed service agreement template and reviewed the Platform's website to ascertain the Company communicates its security objectives and commitments to customers.	No deviations noted.
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.	Inspected the risk management program to ascertain the Company has a defined, formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats.	No deviations noted.
The Information Security Program is reviewed by management annually and approved by the CISO.	Inspected evidence the CISO approved the Information Security Program within the previous 12 months.	No deviations noted.
The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	Inspected the Company's policies and procedures for secure software development to ascertain the purpose is to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	No deviations noted.

Logical and Physical Access Controls

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.		
Control Description	**Tests Performed by MJD**	**Results**
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the compliance management platform monitoring results for a selection of days to ascertain that only authorized users had access to infrastructure and the code repository. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege had been applied.	No deviations noted.
Access to Critical Tools and Resources requires multi-factor authentication.	Inspected the Information Security Program to ascertain the requirement to use multi-factor authentication to access the Company's systems. Inspected the configuration of Critical Tools and Resources to ascertain multi-factor authentication was enforced for all users.	No deviations noted.
System access reviews are performed annually.	Inspected the Company's policies for system access control to ascertain the requirement to perform annual reviews of user access rights. Inspected documentation of the annual system access review, performed during the scope period, and reviewed evidence any findings had been remediated timely, as deemed necessary.	No deviations noted.
The Company's production systems can only be accessed by authorized personnel via an approved encrypted connection (e.g. OpenVPN, SSH, and IP whitelisting associated with AWS Security Groups).	Inspected the Information Security Program to ascertain the requirement for remote access to be strictly controlled with encryption. Inspected the configuration for the production environment to ascertain access is restricted to encrypted channels.	No deviations noted.

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.		
Control Description	**Tests Performed by MJD**	**Results**
Access to migrate changes to production is restricted to authorized individuals with a business need.	Inspected the user access listings and reviewed individuals with the ability to deploy changes to the production environment with management to ascertain privileged access was restricted to appropriate individuals.	No deviations noted.
Management maintains a detailed inventory of all information systems that includes classification and prioritization based on the asset's business value and criticality to the Company.	Inspected the inventory detail to ascertain the Company maintains a detailed inventory of physical and virtual assets.	No deviations noted.
Encryption is used to protect sensitive messaging data at rest.	Inspected the configuration of systems storing sensitive messaging data at rest.	No deviations noted.
Infrastructure resources consist of containerized applications, managed by Kubernetes and built from hardened Docker images, that are subject to vulnerability scanning.	Inspected the CI/CD pipeline and observed the cloud provider administrative console to ascertain infrastructure resources are built from Docker images and subject to vulnerability scanning.	No deviations noted.

Logical and Physical Access Controls

CC6.2: Before 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.		
Control Description	**Tests Performed by MJD**	**Results**
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the compliance management platform monitoring results for a selection of days to ascertain that only authorized users had access to infrastructure and the code repository. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege had been applied.	No deviations noted.
Appropriate management approval is obtained before granting access to Critical Tools and Resources.	Inspected the procedures established to manage access to the Platform to ascertain requirements for access requests to be formally granted or rejected by the appropriate asset owner. Inspected evidence an asset owner approved access to Critical Tools and Resources for a selection of new personnel.	No deviations noted.
System access reviews are performed annually.	Inspected the Company's policies for system access control to ascertain the requirement to perform annual reviews of user access rights. Inspected documentation of the annual system access review, performed during the scope period, and reviewed evidence any findings had been remediated timely, as deemed necessary.	No deviations noted.

CC6.2: Before 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.		
Control Description	**Tests Performed by MJD**	**Results**
Accounts for personnel who have been terminated or no longer require access are disabled within one business day.	Inspected the procedures established to manage access to the Platform to verify employee termination procedures were outlined and included the requirement to disable access within one business day of separation. Inspected the termination checklist for a selection of terminated personnel to ascertain access to Critical Tools and Resources was disabled within the required time frame.	No deviations noted.

Logical and Physical Access Controls

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.		
Control Description	**Tests Performed by MJD**	**Results**
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the compliance management platform monitoring results for a selection of days to ascertain that only authorized users had access to infrastructure and the code repository. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege had been applied.	No deviations noted.
Authentication to Critical Tools and Resources requires a unique username.	Inspected the user listings for Critical Tools and Resources to ascertain each user was assigned a unique username.	No deviations noted.
Appropriate management approval is obtained before granting access to Critical Tools and Resources.	Inspected the procedures established to manage access to the Platform to ascertain requirements for access requests to be formally granted or rejected by the appropriate asset owner. Inspected evidence an asset owner approved access to Critical Tools and Resources for a selection of new personnel.	No deviations noted.
System access reviews are performed annually.	Inspected the Company's policies for system access control to ascertain the requirement to perform annual reviews of user access rights. Inspected documentation of the annual system access review, performed during the scope period, and reviewed evidence any findings had been remediated timely, as deemed necessary.	No deviations 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.		
Control Description	**Tests Performed by MJD**	**Results**
Accounts for personnel who have been terminated or no longer require access are disabled within one business day.	Inspected the procedures established to manage access to the Platform to verify employee termination procedures were outlined and included the requirement to disable access within one business day of separation. Inspected the termination checklist for a selection of terminated personnel to ascertain access to Critical Tools and Resources was disabled within the required time frame.	No deviations noted.

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
The physical security of the Company's primary resources has been outsourced through a cloud-hosting model, and these controls are carved out for the purposes of this report. See Subservice Organizations described within Section 3.

Logical and Physical Access Controls

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.		
Control Description	**Tests Performed by MJD**	**Results**
Accounts for personnel who have been terminated or no longer require access are disabled within one business day.	Inspected the procedures established to manage access to the Platform to verify employee termination procedures were outlined and included the requirement to disable access within one business day of separation. Inspected the termination checklist for a selection of terminated personnel to ascertain access to Critical Tools and Resources was disabled within the required time frame.	No deviations noted.
Management maintains a detailed inventory of all information systems, including classification and prioritization based on the asset's business value and criticality to the Company.	Inspected the inventory detail to ascertain the Company maintains a detailed inventory of physical and virtual assets.	No deviations noted.
Formal data retention and disposal procedures are in place to guide the secure retention and disposal of Company and customer data.	Inspected the Company's Information Security Program to ascertain formal procedures have been established to guide the secure retention and disposal of Company data.	No deviations noted.

Logical and Physical Access Controls

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
Control Description	**Tests Performed by MJD**	**Results**
Logs are aggregated centrally and monitored for indicators of compromise. Alerts are generated based on thresholds established to define potential suspicious activity and are reviewed by the appropriate personnel.	Observed the monitoring dashboard for Grafana to ascertain logs are aggregated centrally and monitored for indicators of compromise. Inspected example alerts to ascertain thresholds were in place to identify potential suspicious activity, and alerts were communicated to appropriate personnel utilizing internal tools.	No deviations noted.
Access to Critical Tools and Resources requires multi-factor authentication.	Inspected the Information Security Program to ascertain the requirement to use multi-factor authentication to access the Company's systems. Inspected the configuration of Critical Tools and Resources to ascertain multi-factor authentication was enforced for all users.	No deviations noted.
The Company's production systems can only be accessed by authorized personnel via an approved encrypted connection (e.g. OpenVPN, SSH, and IP whitelisting associated with AWS Security Groups).	Inspected the Information Security Program to ascertain the requirement for remote access to be strictly controlled with encryption. Inspected the configuration for the production environment to ascertain access is restricted to encrypted channels.	No deviations noted.
Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.	Inspected configurations and other sources of evidence to ascertain the Platform uses secure data protocols consistent with its service commitments and system requirements.	No deviations noted.
A threat detection service is implemented to monitor and detect unauthorized access attempts.	Observed the Amazon GuardDuty dashboard to ascertain continuous monitoring of the Platform’s network was in place to detect security threats, including access anomalies. Observed feed notifications to ascertain personnel are notified when security threats are detected.	No deviations noted.

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
Control Description	**Tests Performed by MJD**	**Results**
Infrastructure resources consist of containerized applications, managed by Kubernetes and built from hardened Docker images, that are subject to vulnerability scanning.	Inspected the CI/CD pipeline and observed the cloud provider administrative console to ascertain infrastructure resources are built from Docker images and subject to vulnerability scanning.	No deviations noted.

CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		
Control Description	**Tests Performed by MJD**	**Results**
Full-disk encryption is implemented for all workstations and laptops.	Inspected monitoring results from the compliance management platform for a selection of personnel to ascertain the individuals utilized computers with full-disk encryption.	No deviations noted.
Encryption is used to protect sensitive messaging data at rest.	Inspected the configuration of systems storing sensitive messaging data at rest.	No deviations noted.
Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.	Inspected configurations and other sources of evidence to ascertain the Platform uses secure data protocols consistent with its service commitments and system requirements.	No deviations noted.
The Company uses firewalls and configures them to protect against threats from sources outside the boundaries of the system. Management reviews its firewall rulesets at least annually, and required changes are tracked to completion.	Inspected the configuration of the firewalls to ascertain the firewall was appropriately deployed to deny all traffic by default unless explicitly allowed. Inspected documentation of the annual firewall review, performed during the scope period, and reviewed evidence any findings had been remediated timely, as deemed necessary.	No deviations noted.
Infrastructure resources consist of containerized applications, managed by Kubernetes and built from hardened Docker images, that are subject to vulnerability scanning.	Inspected the CI/CD pipeline and observed the cloud provider administrative console to ascertain infrastructure resources are built from Docker images and subject to vulnerability scanning.	No deviations noted.

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
Control Description	**Tests Performed by MJD**	**Results**
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company's vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the most recently completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
The Company utilizes Amazon Inspector to continuously scan the environment for software vulnerabilities and unintended network exposure. Alerts are provided to management upon the identification of a vulnerability and are prioritized and remediated according to risk.	Inspected the Amazon Inspector dashboard to ascertain continuous scanning was enabled and reviewed the status of outstanding vulnerabilities with management to determine a process was in place to evaluate and remediate the issues identified.	No deviations noted.
Logs are aggregated centrally and monitored for indicators of compromise. Alerts are generated based on thresholds that have been established to define potential suspicious activity and are reviewed by the appropriate personnel.	Observed the monitoring dashboard for Grafana to ascertain logs are aggregated centrally and monitored for indicators of compromise. Inspected example alerts to ascertain thresholds were in place to identify potential suspicious activity, and alerts were communicated to appropriate personnel utilizing internal tools.	No deviations noted.

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.		
Control Description	**Tests Performed by MJD**	**Results**
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the compliance management platform monitoring results for a selection of days to ascertain that only authorized users had access to infrastructure and the code repository. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege was applied.	No deviations noted.
Personnel accessing Critical Tools and Resources utilize laptops with the most recent operating system security updates and configured with antivirus software.	Inspected monitoring results from the compliance management platform for a selection of personnel to ascertain they utilized computers with the most recent operating system security updates and configured with antivirus software.	No deviations noted.
The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	Inspected the Company's policies and procedures for secure software development to ascertain the purpose is to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	No deviations noted.
Infrastructure resources consist of containerized applications, managed by Kubernetes and built from hardened Docker images, that are subject to vulnerability scanning.	Inspected the CI/CD pipeline and observed the cloud provider administrative console to ascertain infrastructure resources are built from Docker images and subject to vulnerability scanning.	No deviations noted.

System Operations

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.		
Control Description	**Tests Performed by MJD**	**Results**
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company's vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the most recently completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
The Company utilizes Amazon Inspector to continuously scan the environment for software vulnerabilities and unintended network exposure. Alerts are provided to management upon the identification of a vulnerability and are prioritized and remediated according to risk.	Inspected the Amazon Inspector dashboard to ascertain continuous scanning was enabled and reviewed the status of outstanding vulnerabilities with management to determine a process was in place to evaluate and remediate the issues identified.	No deviations noted.
Activity logs and other data sources are analyzed by continuous monitoring tools to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Personnel are assigned to configure the monitoring tools, and the appropriate individuals receive real-time alerts through the generation of emails and other messaging tools.	Observed the dashboard and inspected services provided by cloud monitoring tools to ascertain continuous monitoring had been implemented to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Inspected example alerts identified by cloud monitoring tools and verified notifications are provided to appropriate channels that provide visibility to senior leaders.	No deviations noted.
The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	Inspected the Company's policies and procedures for secure software development to ascertain the purpose is to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	No deviations noted.

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.		
Control Description	**Tests Performed by MJD**	**Results**
Infrastructure resources consist of containerized applications, managed by Kubernetes and built from hardened Docker images, that are subject to vulnerability scanning.	Inspected the CI/CD pipeline and observed the cloud provider administrative console to ascertain infrastructure resources are built from Docker images and subject to vulnerability scanning.	No deviations noted.

CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
Control Description	**Tests Performed by MJD**	**Results**
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company's vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the most recently completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
The Company utilizes Amazon Inspector to continuously scan the environment for software vulnerabilities and unintended network exposure. Alerts are provided to management upon the identification of a vulnerability and are prioritized and remediated according to risk.	Inspected the Amazon Inspector dashboard to ascertain continuous scanning was enabled and reviewed the status of outstanding vulnerabilities with management to determine a process was in place to evaluate and remediate the issues identified.	No deviations noted.
A threat detection service is implemented to monitor and detect unauthorized access attempts.	Observed the Amazon GuardDuty dashboard to ascertain continuous monitoring of the Platform's network was in place to detect security threats, including access anomalies. Observed feed notifications to ascertain personnel are notified when security threats are detected.	No deviations noted.
Identified security deficiencies are tracked and prioritized through internal tools according to their severity.	Observed the dashboard for Asana to ascertain deficiencies are tracked and prioritized to monitor SLAs and provide visibility to senior leaders regarding the timeliness of remediation.	No deviations noted.

CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
Control Description	**Tests Performed by MJD**	**Results**
Activity logs and other data sources are analyzed by continuous monitoring tools to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Personnel are assigned to configure the monitoring tools, and the appropriate individuals receive real-time alerting through the generation of emails and other messaging tools.	Observed the dashboard and inspected services provided by cloud monitoring tools to ascertain continuous monitoring was implemented to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Inspected example alerts identified by cloud monitoring tools and verified notifications are provided to appropriate channels that provide visibility to senior leaders.	No deviations noted.

System Operations

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.		
Control Description	**Tests Performed by MJD**	**Results**
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.	Inspected the Company's vulnerability management policies and procedures to ascertain the requirement to conduct a penetration test of the production environment at least annually. Inspected the most recently completed penetration test report, including evidence of management's review and remediation of high-priority findings, to ascertain the Company completed the penetration test in the last 12 months.	No deviations noted.
The Company utilizes Amazon Inspector to continuously scan the environment for software vulnerabilities and unintended network exposure. Alerts are provided to management upon the identification of a vulnerability and are prioritized and remediated according to risk.	Inspected the Amazon Inspector dashboard to ascertain continuous scanning was enabled and reviewed the status of outstanding vulnerabilities with management to determine a process was in place to evaluate and remediate the issues identified.	No deviations noted.
Identified security deficiencies are tracked and prioritized through internal tools according to their severity.	Observed the dashboard for Asana to ascertain deficiencies are tracked and prioritized to monitor SLAs and provide visibility to senior leaders regarding the timeliness of remediation.	No deviations noted.
The Company has an established plan for incident response that outlines management responsibilities and procedures to respond to information security incidents.	Inspected the Company's policies and plans for incident response to ascertain it outlined the management responsibilities and procedures to respond to information security incidents.	No deviations noted.
Security events are quantified, monitored, and tracked by an identified incident response team, and procedures identified include collecting and preserving information that can serve as evidence.	Inspected the Company's policies and plans for incident response to ascertain the requirements to quantify, monitor, and track potential security incidents and the identification of a formal incident response team. Observed the communication channels integrated with cloud monitoring tools and reviewed example notifications to ascertain the alert was received and the engineering team quantified, monitored, and tracked the event throughout the triage process until resolution and evidence related to the issue were retained.	No deviations noted.

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.		
Control Description	**Tests Performed by MJD**	**Results**
Appropriate communication channels have been established to share the necessary information regarding security events with management, users, and other key individuals.	Inspected the Company's policies and plans for incident response to ascertain it provided guidelines and expectations for communication with management, users, and other key individuals to share the necessary information regarding security events.	No deviations noted.

System Operations

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.		
Control Description	**Tests Performed by MJD**	**Results**
Activity logs and other data sources are analyzed by continuous monitoring tools to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Personnel are assigned to configure the monitoring tools, and the appropriate individuals receive real-time alerts through the generation of emails and other messaging tools.	Observed the dashboard and inspected services provided by cloud monitoring tools to ascertain continuous monitoring was implemented to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Inspected example alerts identified by cloud monitoring tools and verified notifications are provided to appropriate channels that provide visibility to senior leaders.	No deviations noted.
Security events are quantified, monitored, and tracked by an identified incident response team, and procedures identified include collecting and preserving information that can serve as evidence.	Inspected the Company's policies and plans for incident response to ascertain the requirements to quantify, monitor, and track potential security incidents and the identification of a formal incident response team. Observed the communication channels integrated with cloud monitoring tools and reviewed example notifications to ascertain the alert was received and the engineering team quantified, monitored, and tracked the event throughout the triage process until resolution and evidence related to the issue had been retained.	No deviations noted.

CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
Control Description	**Tests Performed by MJD**	**Results**
The Company's plans for incident response require creating, prioritizing, assigning, and tracking follow-ups to completion.	Inspected the Company's policies and plans related to incident response to ascertain the procedures included requirements for creating, prioritizing, and tracking follow-ups to completion. Observed the communication channels integrated with cloud monitoring tools and reviewed example notifications to ascertain the engineering team tracked the event and followed up to completion. Inquired of management and inspected security event documentation to determine that no incidents occurred during the scope period and, thus, the circumstances that would warrant the operation of the control did not occur during the period.	No deviations noted. Circumstances did not warrant operation of incident response controls.

System Operations

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.		
Control Description	**Tests Performed by MJD**	**Results**
Identified security deficiencies are tracked and prioritized through internal tools according to their severity.	Observed the dashboard for Asana to ascertain deficiencies are tracked and prioritized to monitor SLAs and provide visibility to senior leaders regarding the timeliness of remediation.	No deviations noted.
The Company has established plans for incident response that outline management responsibilities and procedures to respond to information security incidents.	Inspected the Company's policies and plans for incident response to ascertain the responsibilities of management had been outlined and procedures were documented to respond to information security incidents.	No deviations noted.
Security events are quantified, monitored, and tracked by an identified incident response team, and procedures identified include collecting and preserving information that can serve as evidence.	Inspected the Company's policies and plans for incident response to ascertain the requirements to quantify, monitor, and track potential security incidents and the identification of a formal incident response team. Observed the communication channels integrated with cloud monitoring tools and reviewed example notifications to ascertain the alert was received and the engineering team quantified, monitored, and tracked the event throughout the triage process until resolution and evidence related to the issue had been retained.	No deviations noted.
Post-mortem meetings are conducted for security incidents to discuss the root causes, remediation steps, and lessons learned.	Inspected the Company's policies and plans related to incident response to ascertain the procedures included requirements for conducting post-mortem meetings for security incidents to discuss the root causes, remediation steps, and lessons learned. Inquired of management and inspected security event documentation to determine that no incidents occurred during the scope period and, thus, the circumstances that would warrant the operation of the control did not occur during the period.	No deviations noted. Circumstances did not warrant operation of incident response controls.

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.		
Control Description	**Tests Performed by MJD**	**Results**
The Company's plans for incident response require creating, prioritizing, assigning, and tracking follow-ups to completion.	Inspected the Company's policies and plans related to incident response to ascertain the procedures included requirements for creating, prioritizing, and tracking follow-ups to completion. Observed the communication channels integrated with cloud monitoring tools and reviewed example notifications to ascertain the engineering team tracked the event and followed up to completion. Inquired of management and inspected security event documentation to determine that no incidents occurred during the scope period and, thus, the circumstances that would warrant the operation of the control did not occur during the period.	No deviations noted. Circumstances did not warrant operation of incident response controls.

Change Management

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.		
Control Description	**Tests Performed by MJD**	**Results**
The Company communicates changes that impact security or user functionality to clients through direct communication via email and the use of a support page that shares release notes and network maintenance windows.	Observed the Company's support page and inspected example communications sent to users to announce product changes to ascertain the Company has channels in place to communicate product releases, bug fixes, and enhancements.	No deviations noted.
Duties and access to sensitive resources are established based on the principle of least privilege.	Inspected the procedures established to manage access to the Platform to ascertain the Company applies the principle of least privilege for determining duties and access levels. Inspected the compliance management platform monitoring results for a selection of days to ascertain that only authorized users had access to infrastructure and the code repository. Inspected the user access listings for Critical Tools and Resources and reviewed access rights with management to ascertain the principle of least privilege was applied.	No deviations noted.
Access to migrate changes to production is restricted to authorized individuals with a business need.	Inspected the user access listings and reviewed individuals with the ability to deploy changes to the production environment with management to ascertain privileged access was restricted to appropriate individuals.	No deviations noted.
The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	Inspected the Company’s policies and procedures for secure software development to ascertain the purpose is to ensure information security is designed and implemented within the development lifecycle for applications and information systems.	No deviations noted.
The Company uses a version control system to manage source code, documentation, release labeling, and other change management tasks.	Inspected configurations and observed the use of version control software to manage source code, documentation, release labeling, and other change management tasks.	No deviations noted.

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.		
Control Description	**Tests Performed by MJD**	**Results**
Releases are tested before deployment, and a release checklist must be completed before deploying code, which includes a checklist of all associated tests.	Inspected the workflow requirements to ascertain the requirement for testing to be performed before deployment.	No deviations noted.
Production and development systems are maintained separately using separate servers and databases.	Inspected evidence that the production environment resources are isolated from development systems.	No deviations noted.
Deployment systems are configured to automatically alert Engineering in Slack for any change to the code repository and any release to the production environment.	Observed the Slack channel to ascertain the integration with the deployment systems was active, and the channel included individuals from Engineering.	No deviations noted.

Risk Mitigation

CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
Control Description	**Tests Performed by MJD**	**Results**
The Company’s plans for business continuity, disaster recovery, and incident response are documented and made available to Company personnel to provide guidance for detecting, responding to, and recovering from security events and incidents.	Inspected the Company's plans for business continuity, disaster recovery, and incident response to ascertain each outlined guidance for detecting, responding to, and recovering from security events and incidents. Observed evidence the Company's plans for business continuity, disaster recovery, and incident response are made available to Company personnel in the compliance management platform.	No deviations noted.
The Company’s risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes consideration of risks arising from potential business disruptions and the identification of mitigation strategies.	Inspected the Risk Assessment Policy to ascertain the requirement for risk assessments to be performed at least annually and includes a consideration of risks arising from potential business disruptions and the identification of mitigation strategies. Inspected the risk assessment to ascertain it was completed in the last 12 months and was performed and documented consistently with the Risk Assessment Policy.	No deviations noted.

Risk Mitigation

CC9.2: The entity assesses and manages risks associated with vendors and business partners.		
Control Description	**Tests Performed by MJD**	**Results**
The vendor management process includes maintaining an inventory of third-party vendors, categorization of vendor risks based on access levels, criticality to services provided and other factors, and a review of the vendor's security, confidentiality, and privacy requirements.	Inspected the Company's policies for vendor management to ascertain procedures include maintaining an inventory of third-party vendors, categorization of vendor risks based on access levels, criticality to services provided and other factors, and a review of the vendor's security and privacy requirements. Obtained the inventory of third-party vendors, reviewed the categorization of vendor risks, and inspected documentation supporting management's review and risk assessment for vendors that store or process data on behalf of customers or perform other high-risk functions related to the Platform.	No deviations noted.
Vendors and business partners are subject to due diligence procedures that include a review of security, confidentiality, and privacy commitments provided through terms of service and written agreements to ensure consistency with the commitments and requirements of the Company.	Inspected evidence of the due diligence procedures performed for vendors that store or process data on behalf of customers or perform other high-risk functions related to the Platform to ascertain each third-party reviewed had been evaluated and was subject to due dilligence procedures performed consistently with the Company's vendor management policies.	No deviations noted.

End of Report