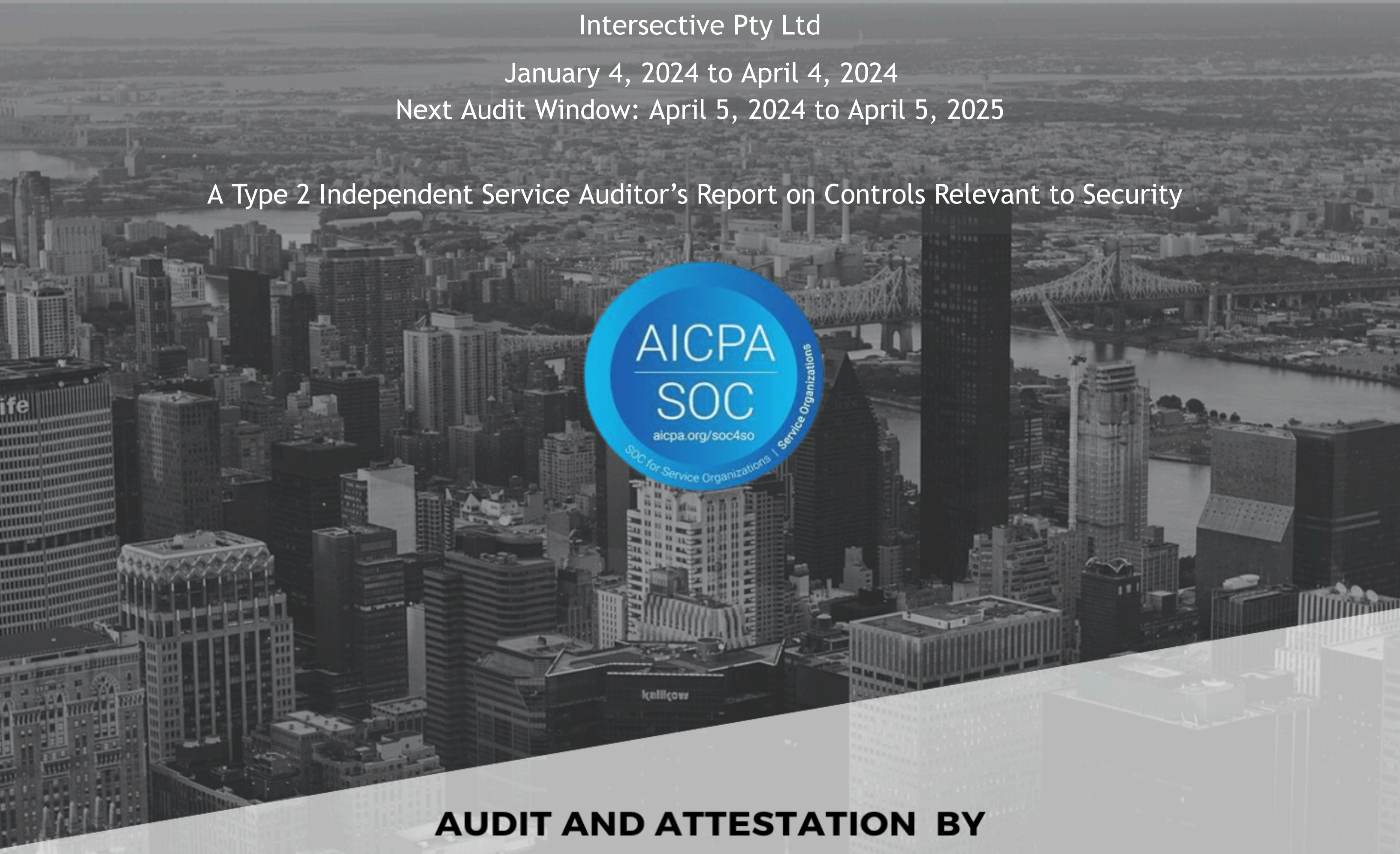
Practera

SOC 2 Type 2 Report

Intersective Pty Ltd

January 4, 2024 to April 4, 2024
Next Audit Window: April 5, 2024 to April 5, 2025

A Type 2 Independent Service Auditor's Report on Controls Relevant to Security



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

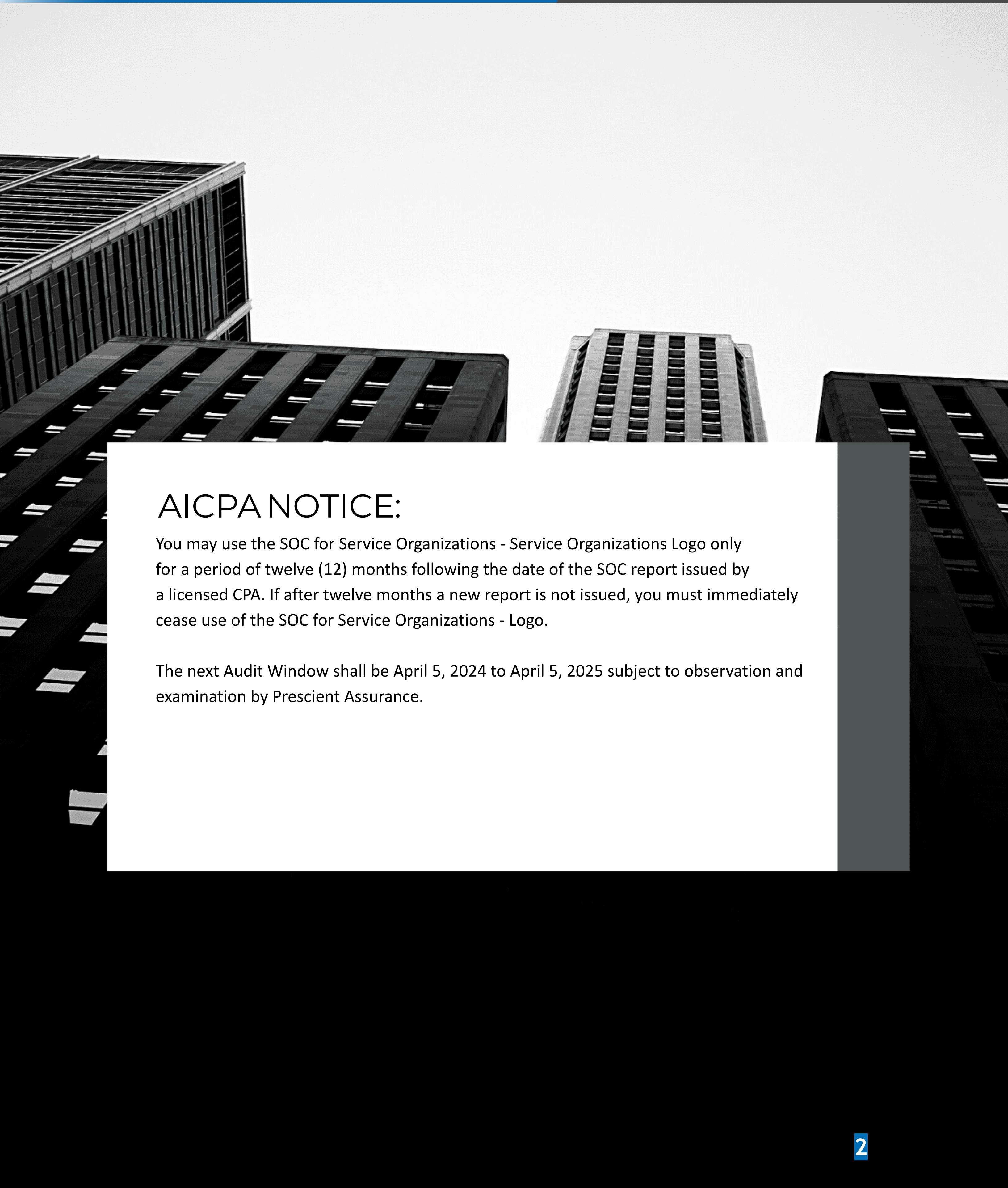
AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA

Prescient Assurance LLC.
1100 Market Street Suite 600
Chattanooga, TN 37402

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319



AICPA NOTICE:

You may use the SOC for Service Organizations - Service Organizations Logo only for a period of twelve (12) months following the date of the SOC report issued by a licensed CPA. If after twelve months a new report is not issued, you must immediately cease use of the SOC for Service Organizations - Logo.

The next Audit Window shall be April 5, 2024 to April 5, 2025 subject to observation and examination by Prescient Assurance.

Table of Contents

SECTION 1

Management's Assertion

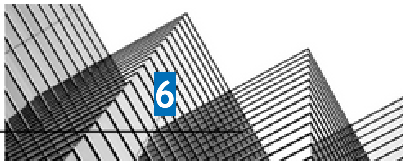
Practera

Management's Assertion

We have prepared the accompanying description of Intersective Pty Ltd's system throughout the period January 4, 2024 to April 4, 2024, 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. The description is intended to provide report users with information about Intersective Pty Ltd's system that may be useful when assessing the risks arising from interactions with Intersective Pty Ltd's system, particularly information about system controls that Intersective Pty Ltd 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*.

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

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



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

a. The description presents Intersective Pty Ltd's system that was designed and implemented throughout the period January 4, 2024 to April 4, 2024 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period January 4, 2024 to April 4, 2024, to provide reasonable assurance that Intersective Pty Ltd'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 organization and user entities applied the complementary controls assumed in the design of Intersective Pty Ltd's controls during that period.
c. The controls stated in the description operated effectively throughout the period January 4, 2024, to April 4, 2024, to provide reasonable assurance that Intersective Pty Ltd's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of Intersective Pty Ltd's controls operated effectively throughout the period.

DocuSigned by:

5296FF6067B84D9...

Suzy Watson

COO

Intersective Pty Ltd

DocuSigned by:

Wes Sonnenreich

BA174E2B880F4E8...

Wes Sonnenreich

CEO / CTO

Intersective Pty Ltd

SECTION 2

Independent Service Auditor's Report

PRESCIENT ASSURANCE

Independent Service Auditor's Report

To: Intersective Pty Ltd

Scope

We have examined Intersective Pty Ltd's ("Intersective Pty Ltd") accompanying description of its Practera system found in Section 3, titled Intersective Pty Ltd System Description throughout the period January 4, 2024, to April 4, 2024, 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, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 4, 2024, to April 4, 2024, to provide reasonable assurance that Intersective Pty Ltd's 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*.

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

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

Service Organization's Responsibilities

Intersective Pty Ltd is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Intersective Pty Ltd's service commitments and system requirements were achieved. In Section 1, Intersective Pty Ltd has provided the accompanying assertion titled "Management's Assertion of Intersective Pty Ltd" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Intersective Pty Ltd 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 Auditors' Responsibilities

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

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

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.

2. 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.

3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.

4. 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.

5. 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.

6. Evaluating the overall presentation of the description.

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

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

Inherent Limitations

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

Opinion

In our opinion, in all material respects:

a. The description presents Intersective Pty Ltd's system that was designed and implemented throughout the period January 4, 2024, to April 4, 2024, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period January 4, 2024, to April 4, 2024, to provide reasonable assurance that Intersective Pty Ltd'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 organization and user entities applied the complementary controls assumed in the design of Intersective Pty Ltd's controls throughout the period.
c. The controls stated in the description operated effectively throughout the period January 4, 2024, to April 4, 2024, to provide reasonable assurance that Intersective Pty Ltd'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 Intersective Pty Ltd's controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of Intersective Pty Ltd, user entities of Intersective Pty Ltd's system during some or all of the period January 4, 2024 to April 4, 2024, business partners of Intersective Pty Ltd subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

1. The nature of the service provided by the service organization.

2. How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.

3. Internal control and its limitations.

4. 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.

5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.

6. The applicable trust services criteria.

7. The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Prescient Assurance LLC

DocuSigned by:
John D Wallace
E5ADEA3569EA450...

John D. Wallace, CPA
Chattanooga, TN
May 22, 2024

SECTION 3

System Description

Practera

DC 1: Company Overview and Types of Products and Services Provided

Company Background

Intersective Pty Ltd is a Experiential Learning Software company. We have developed the Practera Platform which supports 3 party collaboration around experiential learning programs with respect to reflective practice.
We also run large scale authentic experiential programs for adult learners to apply their skills and gain feedback through mentors.
We work with all the Universities in Australia and an increasing number in the UK, Canada and the US.

Description of services overview or services provided

The Practera Platform provides customers with an end to end experiential learning platform design to facilitate the WIL lifecycle of adult learners seeking to apply their knowledge and gain real world feedback. Our platform can be provided just as a platform or we can support turnkey solutions including, design, delivery, facilitation, student recruitment, project recruitment., mentoring and reporting.

The Practera platform focuses on applying a knowledge discipline on a real world project, by reflective practice from learners and scaffolded feedback from industry practitioners. The learning methodology at the core of Practera is the Kolb reflective learning cycle and the platform can be configured for any skills framework.
The platform has 3 different user groups, learners, experts and educators and provides different outputs to the groups to meet their specific requirements from the same experience.

DC 2: The Principal Service Commitments and System Requirements

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

Practera's commitment to customers is communicated via service level agreements, our online Practera Privacy Policy and our terms of services upon user registration

Security commitments

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

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system

- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Up time availability of production systems

DC 3: The Components of the System Used to Provide the Services

The System is comprised of the following components:

- 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 or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

3.1 Primary Infrastructure

Intersective Pty Ltd maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner. To outline the topology of its network, the organization maintains the following network diagram(s).

Hardware	Type	Purpose
Elastic Container Service (ECS)	AWS	Fargate scalable containers run some of our web services
Lambda	AWS	Lambda functions run many of our web services, APIs and internal services
API Gateway	AWS	API Gateway provides an interface to our public API
Elastic Load Balancers	AWS	Load balance internal and external traffic

Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3	AWS	Storage, upload and download of static assets
CloudFront	AWS	Provides caching and network delivery optimization
Aurora Serverless (RDS)	AWS	Scalable database storage for regional data
DynamoDB	AWS	Scalable database storage for global data
ElastiCache	AWS	"Memory" cache service for improved performance
CloudWatch	AWS	Logging of errors and performance metrics

3.2 Primary Software

Intersective Pty Ltd is responsible for managing the development and operation of the Practera Experiential Learning Platform system including infrastructure components such as servers, databases, and storage systems. The in-scope Intersective Pty Ltd infrastructure and software components are shown in the table provided below:

System/Application	Operating System	Purpose
GuardDuty	AWS	Security application used for automated intrusion detection (IDS)
Amazon Web Services	AWS	A range of additional tools such as those used to control access (IAM) and gain insights and analysis (Quicksight) leveraging the infrastructure already on AWS
Asana	Web-based	Internal project management
Employment Hero	Web-based	HR system of record
Filestack	Web-based	Provides a UI for file upload (but not storage)
GitHub	Web-based	Source code repository and associated tools (CI/CD)
Google Drive	Web-based	Main repository for company files
Google Workspace	Web-based	Collaboration platform (email, documents, slides, spreadsheets, storage)
Hubspot	Web-based	Contact and Relationship Management + marketing
Jira	Web-based	Project management for software development lifecycle and ticketing system
Mailchimp	Web-based	API used for transactional mail (mandrill) from Practera platform
Run Powered by ADP	Web-based	US payroll
Slack	Web-based & desktop/mobile	Real-time inter-company communication

Twilio	Web-based	SMS delivery and MFA service (Authy)
Vanta	Web-based	Compliance tracking
XERO	Web-based	Invoice management
Zoom	Web-based	Video conferencing

3.3 People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Intersective Pty Ltd has a staff of approximately 1 organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
This includes:

- Co-CEO Beau Leese (Board Director)
- Co-CEO & CTO Wes Sonnenreich (Board Director)
- Board Director Bill Bartee
- CFO & COO & CRO - Suzy Watson

Operations: Responsible for maintaining the availability of production infrastructure, and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

3.4 Data

Data as defined by Intersective Pty Ltd, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers’ employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized in the following major types of data used by Intersective Pty Ltd

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Intersective Pty Ltd.	● Press releases ● Public website
Internal	Access to internal information is approved by management and is protected from external access.	● Internal memos ● Design documents ● Product specifications ● Correspondences
Customer data	Information received from customers for processing or storage by Intersective Pty Ltd. Intersective Pty Ltd must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	● Customer operating data ● Customer PII ● Customers' customers' PII ● Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Intersective Pty Ltd to operate the business. Intersective Pty Ltd must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	● Legal documents ● Contractual agreements ● Employee PII ● Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Intersective Pty Ltd has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

3.5 Processes and procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention

- Vendor Management

Physical security

Intersective Pty Ltd's production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. Intersective Pty Ltd reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

Logical access

Intersective Pty Ltd provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repartable user provisioning and deprovisioning processes.

Access to these systems are split into admin roles, user roles, and no access roles. User access and roles are reviewed on an annual basis to ensure least privilege access.

Operations is responsible for provision access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Intersective Pty Ltd's policies, completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, Operations is responsible for deprovisioning access to all in scope systems within 72 hours for that employee's termination.

Computer operations - backups

Customer data is backed up and monitored by the Platform for completion and exceptions. If there is an exception, Platform will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer operations - availability

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

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

Intersective Pty Ltd utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open source dependencies and maintains an internal SLA for responding to those issues.

Change management

Intersective Pty Ltd maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

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

Data communications

Intersective Pty Ltd has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Intersective Pty Ltd application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

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

Practera uses several approaches to ensure the security of its systems:

Real-time: We leverage AWS GuardDuty and other AWS security services to ensure the infrastructure is secure. We also regularly monitor platform usage patterns for behaviors that would indicate unauthorized behavior. All end-user systems have active anti-virus/intrusion monitoring either built into the OS or added by third-party services. All reported bugs are analyzed to see if the bugs may have created security risks or data leakage.

At regular intervals: we regularly run vulnerability scans on all of our public facing infrastructure and services to ensure no active critical vulnerabilities exist. Our release process for all hotfixes and features includes several security reviews including code review and, for changes that affect API endpoints, penetration testing on the staging environment. Our staff is regularly reminded to be mindful of phishing and other forms of social engineering attacks. Security and compliance issues are a standing topic of discussion at all leadership meetings.

Boundaries of the system

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

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

DC 4: Disclosures about Identified Security Incidents

No significant incidents have occurred to the services provided to user entities during the review period or since the organization's last review

DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization’s Service Commitments and System Requirements were Achieved

5.1 Integrity and ethical values

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

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

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

5.2 Commitment to competence

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

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

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

5.3 Management's philosophy and operating style

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

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

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

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

5.4 Organizational structure and assignment of authority and responsibility

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

Intersective Pty Ltd's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

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

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

5.5 HR policies and practices

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

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

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

5.6 Risk assessment process

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

5.7 Integration with risk assessment

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

5.8 Information and communication systems

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

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

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

5.9 Monitoring controls

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

5.9.1 On-going Monitoring

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

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

Reporting deficiencies

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

DC 6: Complementary User Entity Controls (CUECs)

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

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

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

DC 7: Complementary Subservice Organization Controls (CSOCs)

Subservice organizations

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

Subservice description of services

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entities services.

Complementary Subservice Organization Controls

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

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

AWS

Category	Criteria	Control
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
Security	CC 6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Security	CC 6.4	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Security	CC 6.4	Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
Security	CC 6.4	Access to server locations is managed by electronic access control devices.

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

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Making regular site visits to vendor and subservice organization(s') facilities
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria That is Not Relevant to the System and the Reasons it is Not Relevant

Criteria not applicable to the system

All Common Criteria/Security, Security criteria were applicable to the Intersective Pty Ltd's Practera Experiential Learning Platform system.

DC 9: Disclosures Of Significant Changes In Last 1 Year

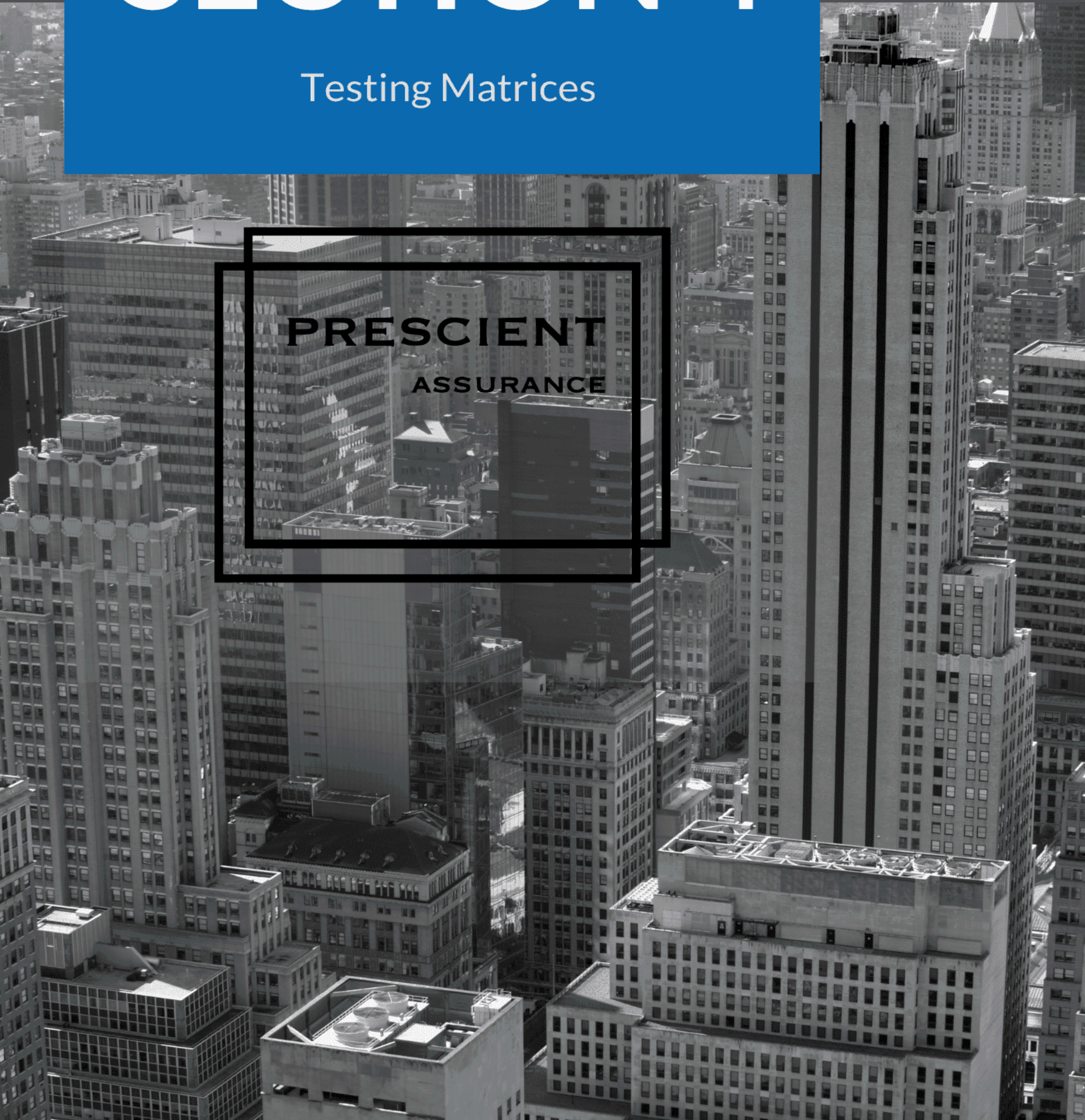
There have been no major vulnerabilities or breaches discovered during the audit period.

In the last year our Platform software has seen significant improvements in functionality and stability. We have removed several third party services to reduce the threat surface and the performance enhancements mitigate a wider range of denial of service attacks.

Six months ago we restructured our Platform team, with the Co-CEO stepping into a full time CTO role to drive a stronger focus on timely delivery of projects including those addressing reliability, scalability and compliance issues, and to improve cross-functional communication between the platform team and the rest of the business. This has also resulted in increased overall business awareness of security and compliance.

SECTION 4

Testing Matrices



PRESCIENT ASSURANCE

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to Practera provided by Intersective Pty Ltd. The scope of the testing was restricted to Practera, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing throughout the period January 04, 2024 to April 04, 2024.

The tests applied to test the Operating Effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that all applicable trust services criteria were achieved during the review date. In selecting the tests of controls, Prescient Assurance LLC considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the control relies on the effectiveness of other controls.
- Whether the control is manually performed or automated.

Types of Tests Generally Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: ● Examination / Inspection of source documentation and authorizations to verify transactions processed. ● Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures. ● Examination / Inspection of systems documentation, configurations, and settings; and ● Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.

Observation	Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed if applicable.

General Sampling Methodology

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Prescient Assurance utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, to determine the number of items to be selected in a sample for a particular test. Prescient Assurance, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

The table below describes the sampling methodology utilized in our testing to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, many times per day	At least 25	**At least 40**
Manual control, daily (Note 1)	At least 25	**At least 40**
Manual control, weekly	At least 5	**At least 10**
Manual control, monthly	At least 3	**At least 4**
Manual control, quarterly	At least 2	**At least 2**
Manual control, annually	Test annually	**Test annually**

Application controls	Test one operation of each relevant aspect of each application control if supported by effective IT general controls; otherwise test at least 15	**Test one operation of each application control if supported by effective IT general controls; otherwise test at least 25**
IT general controls	Follow guidance above for manual and automated aspects of IT general controls	**Follow guidance above for manual and automated aspects of IT general controls**
Notes: 1.) Some controls might be performed frequently, but less than daily. For such controls, the sample size should be interpolated using the above guidance. Generally, for controls where the number of occurrences ranges from 50 to 250 during the year, our minimum sample size using the above table should be approximately 10% of the number of occurrences.		

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

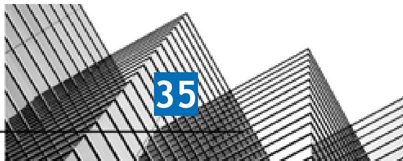
Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than this constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the Operating Effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

Trust ID	COSO Principle	Control Description	Test Applied by the Service Auditor	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.	Inspected the background check reports for a sample of employees hired during the audit period to determine that the company performs background checks on new employees.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected that no contractors were hired during the audit period.	Not tested, did not operate during observation.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the policy acceptance data to determine that the employees hired during the audit period have accepted the Code of Conduct and Human Resource Security Policy upon hire. Moreover, no policy violations were reported during the audit period.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected that no contractors were hired during the audit period.	Not tested, did not operate during observation.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected the signed employment contracts for employees hired during the audit period, showing that confidentiality clause mentioned in the agreements, to determine that the company requires employees to sign a confidentiality agreement during onboarding.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected a log of performance evaluations for a sample of employees to determine that the company managers are required to complete performance evaluations for direct reports at least annually. Observed on a live call completed performance evaluations to determine that the company managers are required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	Inspected the resume of an independent board member to determine that the board includes directors that are independent of the company. Inspected the Board of Directors meeting minutes held in August 2023, to determine that the company's board of directors meets at least annually and maintains formal meeting minutes.	No exceptions noted. No exceptions noted.

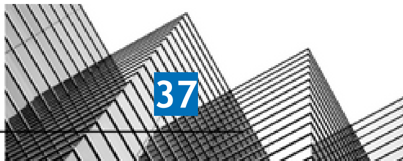
			Inspected that the board of directors meeting was held in August 2023 and is not required to be performed again until August 2024.	Not tested, did not operate during observation.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.	Inspected the profiles of the board members including the CEO, showing their experiences, skills, and qualifications, to determine that the Board of Directors has adequate expertise to lead the management team and oversee the company's internal controls.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	Inspected the minutes of the meeting, held on August 2023, along with Cybersecurity & Privacy Board Discussion notes, dated January 25, 2024, to determine that the company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk and provides feedback and direction to management as needed.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the company's Board of Directors Charter to determine that the company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the company's Board of Directors Charter to determine that the company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of the COO, CTO, CFO, and CEO for the design, development, implementation, and monitoring of security controls have been defined.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the organizational chart showing key positions along with the reporting lines to determine that the company maintains an organizational chart that describes the organizational structure and reporting lines.	No exceptions noted.

CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of the COO, CTO, CFO, and CEO for the design, development, implementation, and monitoring of security controls have been defined. The policy also states the responsibilities of the System Owners, Managers, Co-CEO, Contractors, and employees.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected a log of performance evaluations for a sample of employees to determine that the company managers are required to complete performance evaluations for direct reports at least annually. Observed on a live call completed performance evaluations to determine that the company managers are required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company performs background checks on new employees.	Inspected the background check reports for a sample of employees hired during the audit period to determine that the company performs background checks on new employees.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of the COO, CTO, CFO, and CEO for the design, development, implementation, and monitoring of security controls have been defined. The policy also states the responsibilities of the System Owners, Managers, Co-CEO, Contractors, and employees.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the training completion records to determine that all relevant employees due to complete annual security awareness training within the audit period have completed it. Inspected the onboarding checklists of the employees hired during the observation window showing their security awareness training completion dates to determine that on-hire security awareness training was completed at the time of hire.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the policy acceptance data to determine that the employees hired during the audit period have accepted the Code of Conduct and Human Resource Security Policy upon hire. Moreover, no policy violations were reported during the audit period.	No exceptions noted.



CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of the COO, CTO, CFO, and CEO for the design, development, implementation, and monitoring of security controls have been defined. The policy also states the responsibilities of the System Owners, Managers, Co-CEO, Contractors, and employees.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected a log of performance evaluations for a sample of employees to determine that the company managers are required to complete performance evaluations for direct reports at least annually. Observed on a live call completed performance evaluations to determine that the company managers are required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected that the AWS, Asana, GitHub, Zoom, Slack, Jira, Gsuiteadmin, and Google Drive infrastructures are linked to Vanta to determine that activities on these applications are logged and tracked in Vanta. Inspected that all AWS VPCs have flow logs enabled, all AWS log sinks and server access logs are retained for 365 days, and all accounts have CloudTrail enabled to determine that the company utilizes a log management tool.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Vulnerability scan reports from the audit period showing a list of findings, severity levels, and remediation recommendations, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Moreover, no critical and high vulnerabilities were identified during the scan.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected that the company uses Vanta for continuous self-assessment and monitoring of internal controls to determine that the company performs control self-assessments at least annually.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and	The company requires employees to complete security awareness training	Inspected the training completion records to determine that all relevant employees due to complete annual security awareness	No exceptions noted.

	responsibilities for internal control, necessary to support the functioning of internal control.	within thirty days of hire and at least annually thereafter.	training within the audit period have completed it. Inspected the onboarding checklists of the employees hired during the observation window showing their security awareness training completion dates to determine that on-hire security awareness training was completed at the time of hire.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Inspected an anonymous Google form that allows users to report potential issues or fraud concerns to determine that the company has established an anonymous communication channel for users to report potential issues or fraud concerns.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company communicates system changes to authorized intern al users.	Inspected that the company communicates system changes to authorized internal users via Slack. Inspected that no major system changes besides the platform release were made during the audit period.	No exceptions noted. Not tested, did not operate during observation.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of the COO, CTO, CFO, and CEO for the design, development, implementation, and monitoring of security controls have been defined. The policy also states the responsibilities of the System Owners, Managers, Co-CEO, Contractors, and employees.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Inspected the network architecture diagram to determine that a description of the service delivery process is shared with internal users. Inspected the user guide provided by the company to determine that a description of the company's products is provided online to internal and external users.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of the COO, CTO, CFO, and CEO for the design, development, implementation, and monitoring of security controls have been defined.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal	The company's information security policies and procedures are documented	Inspected the policy list showing that the policies were last updated in May 2023, to determine that the company reviews the policies at least annually.	No exceptions noted.



	control, necessary to support the functioning of internal control.	and reviewed at least annually.	Inspected that policies were last updated in May 2023 to determine that policies are not required to be reviewed until May 2024.	Not tested, did not operate during observation.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, document, and communicate security and data privacy incidents have been documented. Inspected the incident response plan policy acceptance history to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Inspected the network architecture diagram to determine that a description of the service delivery process is shared with internal users. Inspected the user guide provided by the company to determine that a description of the company's products is provided online to internal and external users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company's release notes and user guides on the company's website to determine that the company provides guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the Contact page on the company's website to determine that the company has provided a contact form and a support email for customers to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected vendor agreements for a sample of vendors to determine that the company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting	The company notifies customers of critical system changes that may affect their processing.	Inspected the companies website which included a change log to determine that the company notifies customers of critical	No exceptions noted.

	the functioning of internal control.		system changes that may affect their processing.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected the Terms of Use published on the company's website to determine that the company communicates its commitments regarding security and privacy through its website.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the risk management strategies including risk response and treatment strategies to identify, resolve, and document risks have been described. Inspected a risk assessment report which was completed during the observation window to determine that risk assessments are performed as part of the risk management program.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Management Policy to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
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.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the risk management strategies including risk response and treatment strategies to identify, resolve, and document risks have been described. Inspected a risk assessment report which was completed during the observation window to determine that risk assessments are performed as part of the risk management program.	No exceptions noted.
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.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected a disaster recovery tabletop exercise held during the audit period on January 31, 2024, which included test scenarios, discussion questions, findings, observations, and the company's responses to determine that annual disaster recovery tests are performed at the company.	No exceptions noted.
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.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of	Inspected the risk assessment snapshot dated Jan 10, 2024, to determine that the company's risk assessments are conducted at least annually. Additionally, threats and changes to service commitments are identified and the risks are formally assessed. Inspected the risk register on Vanta to determine that the risk assessment includes a consideration of the potential	No exceptions noted.

		the potential for fraud and how fraud may impact the achievement of objectives.	for fraud and how fraud may impact the achievement of objectives.	
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.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third-party Management Policy to determine that the company ensures that potential risks posed by sharing confidential data are identified, documented, and addressed according to the policy. Inspected the vendor inventory to determine that the company maintains a list of vendors, their risk levels, to their security and privacy commitments.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to 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 assessment snapshot dated Jan 10, 2024, to determine that the company's risk assessments are conducted at least annually. Additionally, threats and changes to service commitments are identified and the risks are formally assessed. Inspected the risk register on Vanta to determine that the risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the risk management strategies including risk response and treatment strategies to identify, resolve, and document risks have been described. Inspected a risk assessment report which was completed during the observation window to determine that risk assessments are performed as part of the risk management program.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the completed StackHawk Penetration testing scan to determine that the company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs. Inspected the completed StackHawk Penetration testing scan to determine that no critical or high vulnerabilities were found.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could	The company's risk assessments are performed at least annually. As part of	Inspected the risk assessment snapshot dated Jan 10, 2024, to determine that the company's risk assessments are conducted	No exceptions noted.

	significantly impact the system of internal control.	this process, threats and changes (environmental, regulatory, and technological) to 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.	at least annually. Additionally, threats and changes to service commitments are identified and the risks are formally assessed. Inspected the risk register on Vanta to determine that the risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected deployments in the GitHub dashboard to determine that the company has a configuration management procedure in place which ensures that system configurations are deployed consistently throughout the environment.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the risk management strategies including risk response and treatment strategies to identify, resolve, and document risks have been described. Inspected a risk assessment report which was completed during the observation window to determine that risk assessments are performed as part of the risk management program.	No exceptions noted.
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.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third-party Management Policy to determine that the company ensures that potential risks posed by sharing confidential data are identified, documented, and addressed according to the policy. Inspected the vendor inventory to determine that the company maintains a list of vendors, their risk levels, to their security and privacy commitments.	No exceptions noted.
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.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the completed StackHawk Penetration testing scan to determine that the company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs. Inspected the completed StackHawk Penetration testing scan to determine that no critical or high vulnerabilities were found.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations	The company performs control self-assessments at least annually to gain	Inspected that the company uses Vanta for continuous self-assessment and monitoring of internal controls to determine that the	No exceptions noted.

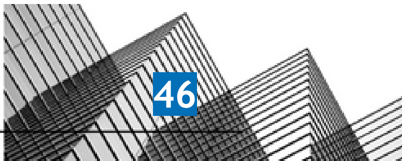
	to ascertain whether the components of internal control are present and functioning.	assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	company performs control self-assessments at least annually.	
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Vulnerability scan reports from the audit period showing a list of findings, severity levels, and remediation recommendations, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Moreover, no critical and high vulnerabilities were identified during the scan.	No exceptions noted.
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.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third-party Management Policy to determine that the company ensures that potential risks posed by sharing confidential data are identified, documented, and addressed according to the policy. Inspected the vendor inventory to determine that the company maintains a list of vendors, their risk levels, to their security and privacy commitments.	No exceptions noted.
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.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected that the company uses Vanta for continuous self-assessment and monitoring of internal controls to determine that the company performs control self-assessments at least annually.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the policy list showing that the policies were last updated in May 2023, to determine that the company reviews the policies at least annually. Inspected that policies were last updated in May 2023 to determine that policies are not required to be reviewed until May 2024.	No exceptions noted. Not tested, did not operate during observation.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and	Inspected the Risk Management Policy to determine that the risk management strategies including risk response and treatment strategies to identify, resolve, and document risks have been described. Inspected a risk assessment report which was completed during the observation window to determine that risk assessments	No exceptions noted.

		mitigation strategies for those risks.	are performed as part of the risk management program.	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the policy list showing that the policies were last updated in May 2023, to determine that the company reviews the policies at least annually. Inspected that policies were last updated in May 2023 to determine that policies are not required to be reviewed until May 2024.	No exceptions noted. Not tested, did not operate during observation.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine that the company has described secure system engineering principles, change control procedures, and version control guidelines.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy to determine that the company has established access control procedures, including access provisioning, de-provisioning, access change, and review procedures.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Information Management Policy to determine that the company has defined the procedures for retaining and disposing of customer data.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Operations Security Policy to determine that information backup requirements have been documented stating that backup copies are required to be taken regularly and restore capabilities are required to be tested periodically, not less than annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected a sample of change tickets, Zephyr Scale automated testing, and slack channel pertaining to changes to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.

CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine that the company has described secure system engineering principles, change control procedures, and version control guidelines.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the policy list showing that the policies were last updated in May 2023, to determine that the company reviews the policies at least annually. Inspected that policies were last updated in May 2023 to determine that policies are not required to be reviewed until May 2024.	No exceptions noted. Not tested, did not operate during observation.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of the COO, CTO, CFO, and CEO for the design, development, implementation, and monitoring of security controls have been defined. The policy also states the responsibilities of the System Owners, Managers, Co-CEO, Contractors, and employees.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third-party Management Policy to determine that the company ensures that potential risks posed by sharing confidential data are identified, documented, and addressed according to the policy. Inspected the vendor inventory to determine that the company maintains a list of vendors, their risk levels, to their security and privacy commitments.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, document, and communicate security and data privacy incidents have been documented. Inspected the incident response plan policy acceptance history to determine that the company has security and privacy incident response policies and procedures that are	No exceptions noted.

			documented and communicated to authorized users.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Management Policy to determine that the company specifies its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the risk management strategies including risk response and treatment strategies to identify, resolve, and document risks have been described. Inspected a risk assessment report which was completed during the observation window to determine that risk assessments are performed as part of the risk management program.	No exceptions 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.	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.	Inspected that MFA is enabled on GitHub, AWS, and Google Workspace accounts except those that are service accounts, along with screenshots showing authentication code prompts for accessing AWS, GitHub, and Google Workspace accounts, to determine that the company requires authentication to production datastores to use authorized secure authentication mechanisms.	No exceptions 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.	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the AWS Administrator listing to determine that the company restricts privileged access to encryption keys to authorized users with a business need.	No exceptions 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.	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the AWS Administrator listing to determine that the company restricts privileged access to the firewall to authorized users with a business need.	No exceptions 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.	The company restricts privileged access to the operating system to authorized users with a business need.	Inspected the AWS administrator listing to determine the company restricts privileged access to the operating system to authorized users with a business need.	No exceptions 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.	The company restricts privileged access to the production network to authorized users with a business need.	Inspected a list of users accessing AWS, GitHUb, Google Workspace accounts to determine that the company restricts privileged access to the production network to authorized users with a business need.	No exceptions 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.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the system access request log to determine that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	No exceptions 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.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy to determine that the company has established access control procedures, including access provisioning, de-provisioning, access change, and review procedures.	No exceptions 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.	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the Network Segregation Plan showing segregation with security groups, public and private subnets, along with separate production and testing environment VPCs, to determine that the company's network was segmented to prevent unauthorized access to customer data.	No exceptions 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.	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the AWS User listing to determine that the company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	No exceptions 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.	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the password Requirements and MFA Configurations for AWS, Google Workspace, Github, Jira, and HubSpot to determine that the company requires passwords for in-scope system components to be configured according to the company's policy.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets	The company's production systems can only be remotely accessed by authorized employees possessing a valid	Inspected that MFA is enabled on AWS, HubSpot. GitHub, and Workspace accounts except those that are service accounts to determine that the company's production systems can only be remotely accessed by	No exceptions noted.



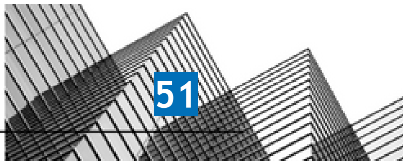
	to protect them from security events to meet the entity's objectives.	multi-factor authentication (MFA) method.	authorized employees possessing a valid multi-factor authentication (MFA) method.	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's datastores housing sensitive customer data are encrypted at rest.	Inspected that AWS DynamoDB Tables are encrypted to determine that the company's data stores housing sensitive customer data are encrypted at rest.	No exceptions 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.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the Information Management Policy and procedures to determine that the company has documented the classification of information is classified along with the internal retention and disposal procedures for the company's managed accounts and devices.	No exceptions 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.	The company restricts access to migrate changes to production to authorized personnel.	Inspected the listing of GitHub administrators to determine that the company restricts access to migrate changes to production to authorized personnel.	No exceptions 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.	The company maintains a formal inventory of production system assets.	Inspected the asset inventory on Vanta to determine that the company maintains an inventory of Container repositories, Storage buckets, and Git repositories, among other production system assets.	No exceptions 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.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Google Workspace MFA Status, GitHub MFA Configurations, and AWS Configurations to determine that the company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions 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.	The company restricts privileged access to the application to authorized users with a business need.	Inspected a list of users with the privileged access to AWS, GitLab and Google Workspace, along with their respective roles to determine that the company restricts privileged access to the application to authorized users only.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure,	The company restricts privileged access to	Inspected a list of users accessing AWS, GitHUb, and Google Workspace accounts, to determine that the company restricts	No exceptions noted.

	and architectures over protected information assets to protect them from security events to meet the entity's objectives.	databases to authorized users with a business need.	privileged access to databases to authorized users with a business need.	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the security certificate on the company's website which is valid until May 16, 2024, to determine that remote access to the company's website required an encrypted connection. Inspected the Session Manager Configurations and Session Manager Logs to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the completed access review from Q1 2024 to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy to determine that the company has established access control procedures, including access provisioning, de-provisioning, access change, and review procedures.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the offboarding checklist of an employee terminated during the audit period to determine that access was revoked for terminated employees within the SLA.	No exceptions noted.

	when user access is no longer authorized.			
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Google Workspace MFA Status, GitHub MFA Configurations, and AWS Configurations to determine that the company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the system access request log to determine that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Google Workspace MFA Status, GitHub MFA Configurations, and AWS Configurations to determine that the company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the offboarding checklist of an employee terminated during the audit period to determine that access was revoked for terminated employees within the SLA.	No exceptions noted.

CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the completed access review from Q1 2024 to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the system access request log to determine that the company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy to determine that the company has established access control procedures, including access provisioning, de-provisioning, access change, and review procedures.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the completed access review from Q1 2024 to determine that the company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the offboarding checklist of an employee terminated during the audit period to determine that access was revoked for terminated employees within the SLA.	No exceptions noted.

CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Information Management Policy to determine that the company has defined the procedures for retaining and disposing of customer data.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inquires with the company to determine that no customer left the company services during the audit period.	Not tested, did not operate during observation.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the security certificate on the company's website which is valid until May 16, 2024, to determine that remote access to the company's website required an encrypted connection. Inspected the Session Manager Configurations and Session Manager Logs to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Google Workspace MFA Status, GitHub MFA Configurations, and AWS Configurations to determine that the company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the GuardDuty Dashboard to determine that the company is using AWS GuardDuty as an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected the AWS Security Configuration report review from January 2024, which discusses the firewall usage, and found that the company utilizes the AWS cloud infrastructure, including its built-in firewall feature. This review confirms that the company conducts annual reviews of its firewall rulesets, and no changes were identified during the latest review.	No exceptions noted.



CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses firewalls and configures them to prevent unauthorized access.	Inspected the company's firewall configurations in AWS to determine that the company has configured firewalls to prevent unauthorized access.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected vulnerability scans from January 9, 2024 to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. Inspected the vulnerability scans from January 9, 2024 to determine that no critical or high vulnerabilities were identified.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the AWS Well-Architected Framework from the audit period to determine that the company uses AWS Well-architected framework for security.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the security certificate of the company's website, valid up to May 16, 2024, to determine that the company accepts TLS connections using up-to-date cipher suites, and redirects HTTP to HTTPS via a 3XX status code.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected that MFA is enabled on AWS, HubSpot. GitHub, and Workspace accounts except those that are service accounts to determine that the company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the security certificate of the company's website, valid up to May 16, 2024, to determine that the company accepts TLS connections using up-to-date cipher suites, and redirects HTTP to HTTPS via a 3XX status code.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected that the company uses Vanta as an MDM to determine that the company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	No exceptions noted.

	meet the entity's objectives.			
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.	The company encrypts portable and removable media devices when used.	Inspected that all employee workstations with the Vanta Agent installed and have encrypted hard drives. Inspected that the company does not own any portable or removable media devices.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine that the company has described secure system engineering principles, change control procedures, and version control guidelines.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected vulnerability scans from January 9, 2024 to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. Inspected the vulnerability scans from January 9, 2024 to determine that no critical or high vulnerabilities were identified.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected a list of employee workstations to determine that the relevant employees' workstations have antivirus software installed.	No exceptions 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.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected deployments in the GitHub dashboard to determine that the company has a configuration management procedure in place which ensures that system configurations are deployed consistently throughout the environment.	No exceptions 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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Vulnerability scan reports from the audit period showing a list of findings, severity levels, and remediation recommendations, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Moreover, no critical and high vulnerabilities were identified during the scan.	No exceptions 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.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to 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 assessment snapshot dated Jan 10, 2024, to determine that the company's risk assessments are conducted at least annually. Additionally, threats and changes to service commitments are identified and the risks are formally assessed. Inspected the risk register on Vanta to determine that the risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No exceptions 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.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected a sample of change tickets, Zephyr Scale automated testing, and slack channel pertaining to changes to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions 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.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the Operations Security Policy to determine that technical vulnerability management and system monitoring and logging procedures have been established and the Engineering departments are responsible for evaluating the severity of vulnerabilities.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Vulnerability scan reports from the audit period showing a list of findings, severity levels, and remediation recommendations, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Moreover, no critical and high vulnerabilities were identified during the scan.	No exceptions noted.

CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the GuardDuty Dashboard to determine that the company is using AWS GuardDuty as an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected that all AWS accounts have at least one load balancer in use except those that are dedicated for Global services, all external AWS load balancers redirect HTTP traffic to HTTPS, and that latency, errors and host health for all AWS load balancers, AWS DynamoDB tables, AWS Lambda functions and SQS Queues have CloudWatch alarm enabled to determine that infrastructure monitoring is in place and alerts are generated when required.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected that the AWS, Asana, GitHub, Zoom, Slack, Jira, Gsuiteadmin, and Google Drive infrastructures are linked to Vanta to determine that activities on these applications are logged and tracked in Vanta. Inspected that all AWS VPCs have flow logs enabled, all AWS log sinks and server access logs are retained for 365 days, and all accounts have CloudTrail enabled to determine that the company utilizes a log management tool.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the Operations Security Policy to determine that technical vulnerability management and system monitoring and logging procedures have been established and the Engineering departments are responsible for evaluating the severity of vulnerabilities.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate	Inspected the completed StackHawk Penetration testing scan to determine that the company's penetration testing is performed at least annually. A remediation plan is developed and changes are	No exceptions noted.

	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.	vulnerabilities in accordance with SLAs.	implemented to remediate vulnerabilities in accordance with SLAs. Inspected the completed StackHawk Penetration testing scan to determine that no critical or high vulnerabilities were found.	
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected vulnerability scans from January 9, 2024 to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. Inspected the vulnerability scans from January 9, 2024 to determine that no critical or high vulnerabilities were identified.	No exceptions 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.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the incident response plan to determine that the company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. Inquired of the company to determine that no incidents occurred within the observation window.	No exceptions noted. Not tested, did not operate during observation.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, document, and communicate security and data privacy incidents have been documented. Inspected the incident response plan policy acceptance history to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the	Inspected vulnerability scans from January 9, 2024 to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security	No exceptions noted.

	communicate security incidents, as appropriate.	service are hardened against security threats.	threats. Inspected the vulnerability scans from January 9, 2024 to determine that no critical or high vulnerabilities were identified.	
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Vulnerability scan reports from the audit period showing a list of findings, severity levels, and remediation recommendations, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Moreover, no critical and high vulnerabilities were identified during the scan.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, document, and communicate security and data privacy incidents have been documented. Inspected the incident response plan policy acceptance history to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company tests their incident response plan at least annually.	Inspected the disaster recovery tabletop exercise held during the audit period on January 31, 2024, which included test incident scenarios and the company's responses to determine that the company tests the incident response plan at least annually.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the incident response plan to determine that the company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. Inquired of the company to determine that no incidents occurred within the observation window.	No exceptions noted. Not tested, did not operate during observation.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company tests their incident response plan at least annually.	Inspected the disaster recovery tabletop exercise held during the audit period on January 31, 2024, which included test incident scenarios and the company's	No exceptions noted.

			responses to determine that the company tests the incident response plan at least annually.	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the incident response plan to determine that the company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. Inquired of the company to determine that no incidents occurred within the observation window.	Not tested, did not operate during observation.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, document, and communicate security and data privacy incidents have been documented. Inspected the incident response plan policy acceptance history to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected a disaster recovery tabletop exercise held during the audit period on January 31, 2024, which included test scenarios, discussion questions, findings, observations, and the company's responses to determine that annual disaster recovery tests are performed at the company.	No exceptions 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.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected a sample of change tickets, Zephyr Scale automated testing, and slack channel pertaining to changes to determine that the company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions 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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected vulnerability scans from January 9, 2024 to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. Inspected the vulnerability scans from	No exceptions noted.

			January 9, 2024 to determine that no critical or high vulnerabilities were identified.	
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Vulnerability scan reports from the audit period showing a list of findings, severity levels, and remediation recommendations, to determine that host-based vulnerability scans are performed at least quarterly on all external-facing systems. Moreover, no critical and high vulnerabilities were identified during the scan.	No exceptions 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.	The company restricts access to migrate changes to production to authorized personnel.	Inspected the listing of GitHub administrators to determine that the company restricts access to migrate changes to production to authorized personnel.	No exceptions 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.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the completed StackHawk Penetration testing scan to determine that the company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs. Inspected the completed StackHawk Penetration testing scan to determine that no critical or high vulnerabilities were found.	No exceptions 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.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine that the company has described secure system engineering principles, change control procedures, and version control guidelines.	No exceptions 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.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the AWS Well-Architected Framework from the audit period to determine that the company uses AWS Well-architected framework for security.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks	The company has a documented risk management program in	Inspected the Risk Management Policy to determine that the risk management strategies including risk response and	No exceptions noted.

	arising from potential business disruptions.	place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	treatment strategies to identify, resolve, and document risks have been described. Inspected a risk assessment report which was completed during the observation window to determine that risk assessments are performed as part of the risk management program.	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to 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 assessment snapshot dated Jan 10, 2024, to determine that the company's risk assessments are conducted at least annually. Additionally, threats and changes to service commitments are identified and the risks are formally assessed. Inspected the risk register on Vanta to determine that the risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the communications and escalation plan with roles and responsibilities of key personnel and business continuity strategies for critical services have been described.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected the liability insurance certificate by Acord, which is valid until October 06, 2024, to determine that the company has maintained cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected vendor agreements for a sample of vendors to determine that the company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical	Inspected the Third-party Management Policy to determine that the company ensures that potential risks posed by sharing confidential data are identified, documented, and addressed according to the policy. Inspected the vendor inventory to determine that the company maintains a	No exceptions noted.

		third-party vendors at least annually.	list of vendors, their risk levels, to their security and privacy commitments.	