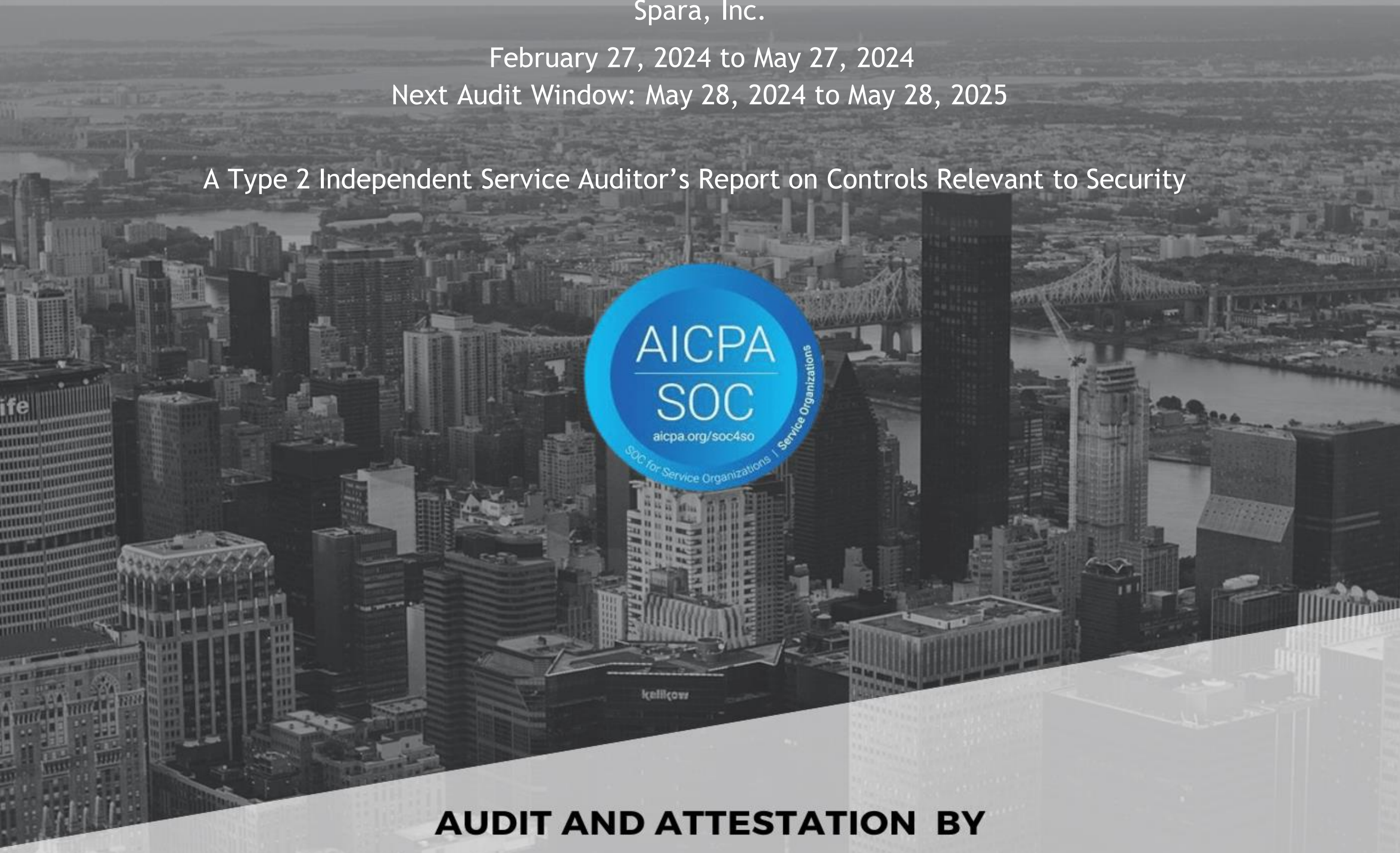


SOC 2 Type 2 Report

Spara, Inc.

February 27, 2024 to May 27, 2024
Next Audit Window: May 28, 2024 to May 28, 2025

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

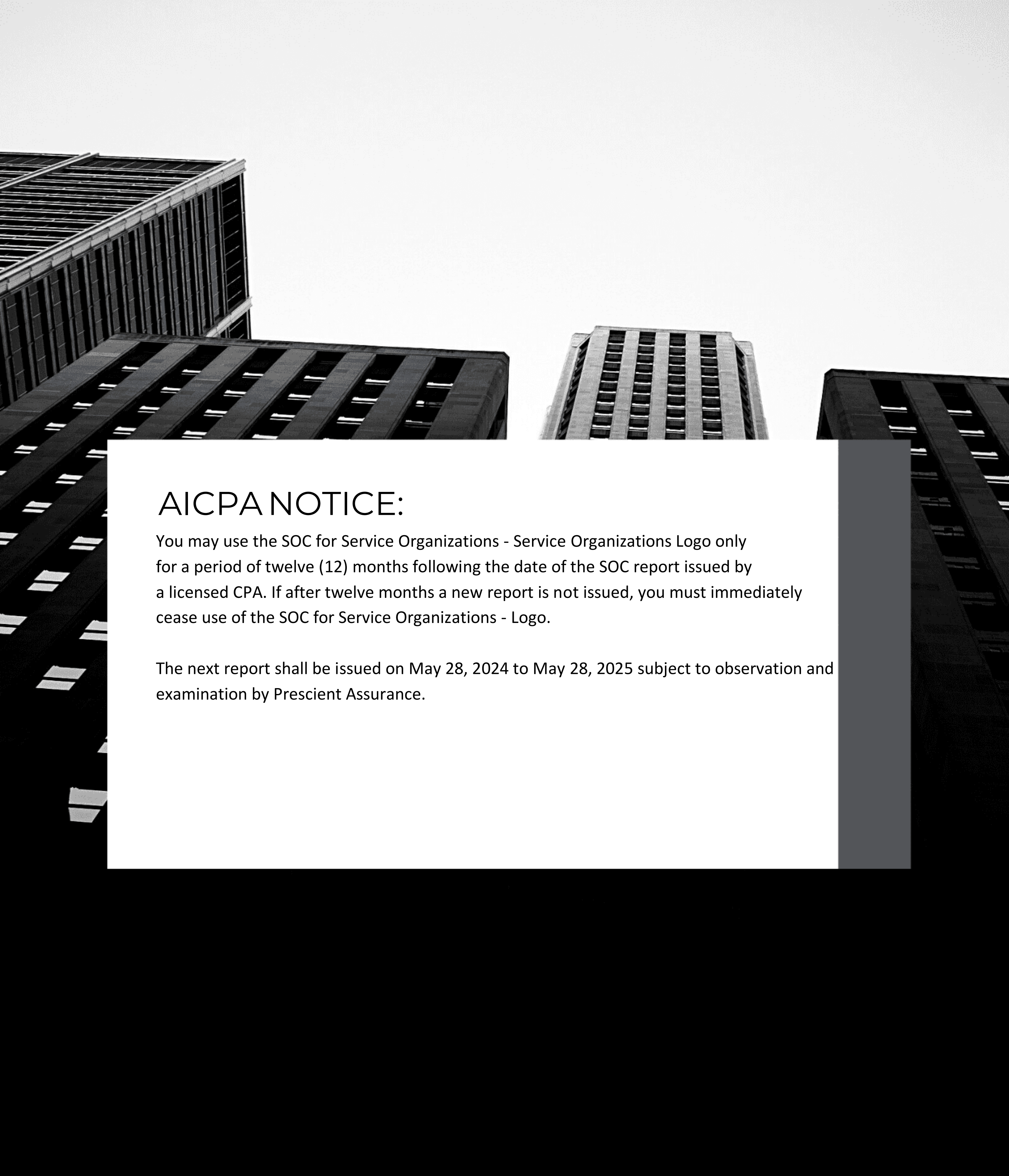
AUDIT AND ATTESTATION BY

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 report shall be issued on May 28, 2024 to May 28, 2025 subject to observation and examination by Prescient Assurance.

Table of Contents

SECTION 1

Management's Assertion

spara

Management's Assertion

We have prepared the accompanying description of Spara, Inc.'s system throughout the period February 27, 2024 to May 27, 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 Spara, Inc.'s system that may be useful when assessing the risks arising from interactions with Spara, Inc.'s system, particularly information about system controls that Spara, Inc. 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*.

Spara, Inc. 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 Spara, Inc., to achieve Spara, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Spara, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Spara, Inc.'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 Spara, Inc., to achieve Spara, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Spara, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Spara, Inc.'s controls.

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

a. The description presents Spara, Inc.'s system that was designed and implemented throughout the period February 27, 2024 to May 27, 2024 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period February 27, 2024 to May 27, 2024, to provide reasonable assurance that Spara, Inc.'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 Spara, Inc.'s controls during that period.
c. The controls stated in the description operated effectively throughout the period February 27, 2024, to May 27, 2024, to provide reasonable assurance that Spara, Inc.'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 Spara, Inc.'s controls operated effectively throughout the period.

DocuSigned by:
Alexander Pease
3F440D315033440...

Alexander Pease
CTO
Spara, Inc.

SECTION 2

Independent Service Auditor's Report

PRESCIENT
ASSURANCE

Independent Service Auditor's Report

To: Spara, Inc.

Scope

We have examined Spara, Inc.'s ("Spara, Inc.") accompanying description of its Spara system found in Section 3, titled Spara, Inc. System Description throughout the period February 27, 2024, to May 27, 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 February 27, 2024, to May 27, 2024, to provide reasonable assurance that Spara, Inc.'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*.

Spara, Inc. 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 Spara, Inc., to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Spara, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Spara, Inc.'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 Spara, Inc., to achieve Spara, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Spara, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Spara, Inc.'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

Spara, Inc. 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 Spara, Inc.'s service commitments and system requirements were achieved. In Section 1, Spara, Inc. has provided the accompanying assertion titled "Management's Assertion of Spara, Inc." (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Spara, Inc. is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the 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 Spara, Inc.'s system that was designed and implemented throughout the period February 27, 2024, to May 27, 2024, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period February 27, 2024, to May 27, 2024, to provide reasonable assurance that Spara, Inc.'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 Spara, Inc.'s controls throughout the period.
c. The controls stated in the description operated effectively throughout the period February 27, 2024, to May 27, 2024, to provide reasonable assurance that Spara, Inc.'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 Spara, Inc.'s controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of Spara, Inc., user entities of Spara, Inc.’s system during some or all of the period February 27, 2024 to May 27, 2024, business partners of Spara, Inc. 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
F5ADFA3569EA450...

John D. Wallace, CPA
Chattanooga, TN
June 28, 2024

SECTION 3

System Description

spara

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

Spara, Inc. (the "company") was founded on December 22nd, 2024 by Alexander David Walker and Alexader Pease to provide a SaaS-based solution to high volume sales touchpoints for complex products. The organization is based out of New York, NY.

Spara, Inc.'s core product, Spara (the "system") is a Software as a Service (SaaS) solution that includes the following services:

- Buyer-facing interface for multimodal sales conversations
- User-facing platform for managing the performance of these interactions

DC 2: The Principal Service Commitments and System Requirements

Spara, Inc. designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Spara, Inc. makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Spara, Inc. has established for the services. The system services are subject to the Security, Confidentiality, and Availability commitments established internally for its services. Commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

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;
- 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
- Uptime availability of production systems

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

The System description is comprised of the following components:

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

programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications 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 Software

Primary Software		
Hardware	**Type**	**Purpose**
Heroku	Heroku Platform	Container runtime for web services, APIs, workers, schedulers. Includes right-scaling and self-heading to replace failed containers.
Heroku	Heroku Pipelines	CI/CS system to produce containers from source code and buildpacks and deploy containers to staging and production environments.
Heroku	Heroku Postgres	Primary transactional database, encryption at rest, and automatic backups.

3.2 Primary Infrastructure

Primary Infrastructure		
System/Application	**Operating System**	**Purpose**
Python	Linux	Primary development language/runtime for applications
PostgreSQL	Linux	Transactional database

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.

Spara, Inc. has a staff of approximately 3 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.

CEO - Alexander David Walker
CTO - Alexander Pease
VP of Software Engineering - Yoni Baciu

3.4 Data

Data as defined by Spara, Inc., constitutes the following:

- Customer production-level data stored in a hosted PostgreSQL environment.
- Customer communications via Google Apps email or Slack.
- Customer-submitted data via communication channels stored in Google Drive. Data is categorized in four major types of data used by Spara, Inc.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Spara, Inc.	● 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 Spara, Inc. Spara, Inc. 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 Spara, Inc. to operate the business. Spara, Inc. 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, Spara, Inc. 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 Alexander Pease. 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

3.5.1 Physical Security

Spara, Inc.'s production servers are maintained by Heroku. The physical and environmental security protections are the responsibility of Heroku.

3.5.2 Logical Access

Spara, Inc. 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 three levels; Administrator, User, and No Access. User access and roles are reviewed on an annual basis to ensure least privilege access.

Management is responsible for provisioning access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Spara, Inc.'s policies, completing security training. These steps must be completed within 3 days of hire.

When an employee is terminated, Management is responsible for deprovisioning access to all in scope systems within 3 days for that employee's termination.

3.5.3 Computer Operations - Backups

Customer data is backed up and monitored by the Engineering team / Alexander Pease for completion and exceptions. If there is an exception Engineering team / Alexander Pease 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 Heroku. Backups are encrypted, with access restricted to key personnel.

3.5.4 Computer Operations - Availability

Spara, Inc. 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.

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

Spara, Inc. 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.

3.5.5 Change Management

Spara, Inc. 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.

3.5.6 Data Communications

Spara, Inc. 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 Spara, Inc. 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.

3.3 Boundaries of the System

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

DC 4: Disclosures about Identified Security Incidents

No significant incidents have occurred to the services provided to user entities in the last 3 months preceding the end of the review date.

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 Spara, Inc.'s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Spara, Inc.'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

Spara, Inc.'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.

MANAGEMENT'S PHILOSOPHY AND OPERATING STYLE

The Spara, Inc. 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 Spara, Inc. 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 Spara, Inc. 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.

5.3 Organizational Structure and Assignment of Authority and Responsibility

Spara, Inc.'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.

Spara, Inc.'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.

5.4 Human Resource Policies and Practices

Spara, Inc.'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. Spara, Inc.'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 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.

5.5 Risk Assessment Process

Spara, Inc.'s risk assessment process identifies and manages risks that could potentially affect Spara, Inc.'s ability to provide reliable and secure services to our customers. As part of this process, Spara, Inc. 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 Spara, Inc. product development process so they can be dealt with predictably and iteratively.

5.6 Integration with Risk Assessment

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

5.7 Information and Communication Systems

Information and communication are an integral component of Spara, Inc.'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.

Spara, Inc. uses several information and communication channels internally to share information with management, employees, contractors, and customers. Spara, Inc. 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, Spara, Inc. uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

5.8 Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Spara, Inc.'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.

5.8.1 On-going Monitoring

Spara, Inc.'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 Spara, Inc.'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 Spara, Inc.'s personnel.

5.9 Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing 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)

Spara, Inc.'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 Spara, Inc.'s services to be solely achieved by Spara, Inc. control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Spara, Inc.'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 Spara, Inc.
- User entities are responsible for notifying Spara, Inc. of changes made to technical or administrative contact information.
- User entities are responsible for maintaining their own system(s) of record for business activities unrelated to Spara's stated purpose(s).
- User entities are responsible for ensuring the supervision, management, and control of the use of Spara, Inc. 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 Spara, Inc. services.
- User entities are responsible for immediately notifying Spara, Inc. 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

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

Heroku		
Category	**Criteria**	**Control**
Security	CC6.4	Only authorized personnel have access to the facilities housing the system.
Security	CC6.4	Badge access control systems are in place in order to access the facilities.
Security	CC6.4	Visitor access to the corporate facility and data center are recorded in visitor access logs
Security	CC6.4	Visitors are required to wear a visitor badge while onsite at the facilities.

Security	CC6.4	Visitors are required to check in with security and show a government issued ID prior to being granted access to the facilities
Security	CC6.4	Visitors are required to have an escort at all times.

DC 8: Trust Services Criterion not Relevant to the System and Reasons

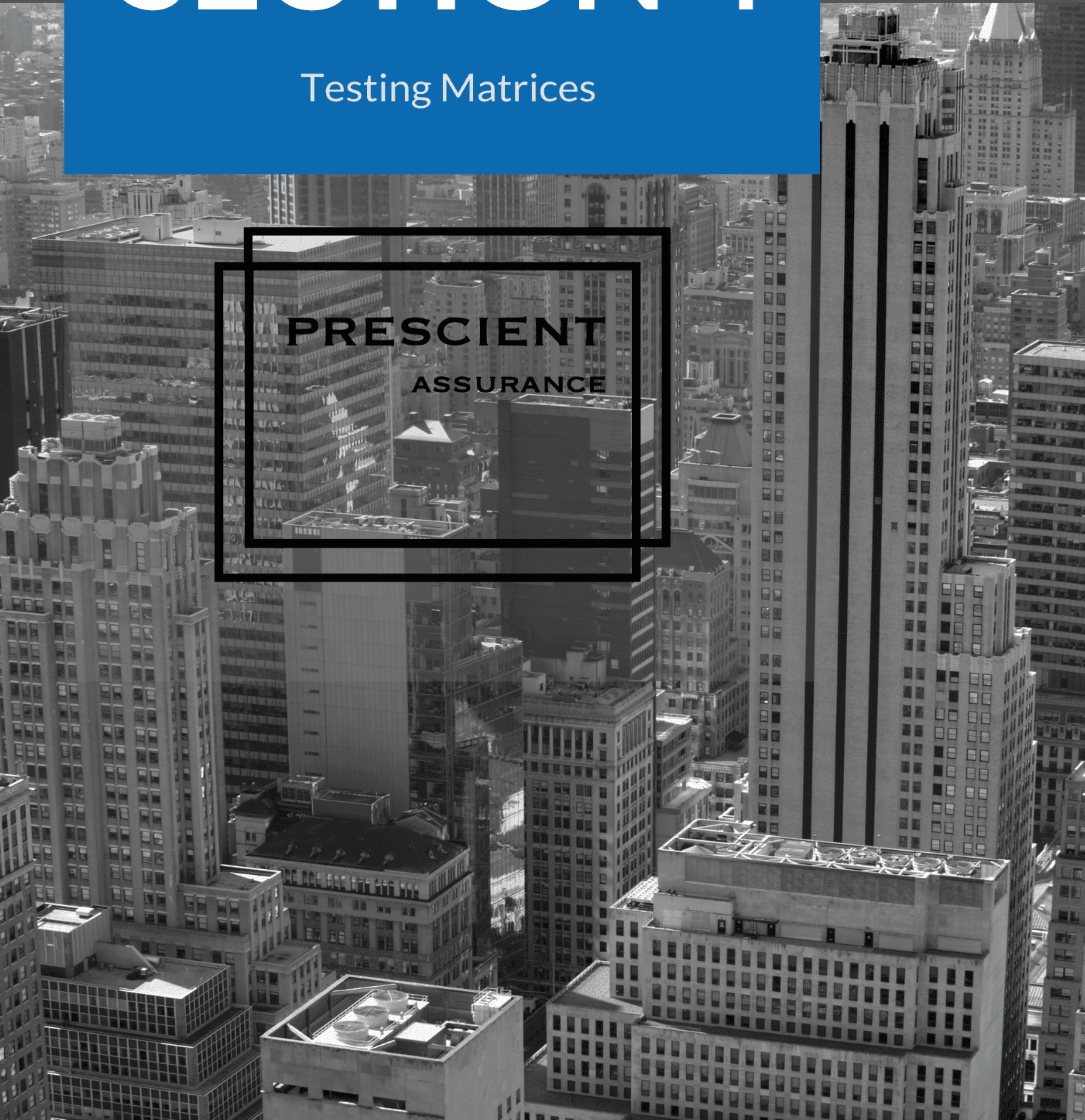
All Common Criteria/Security criteria were applicable to the Spara, Inc. Spara platform.

DC 9: Disclosure of Significant Changes in Last 1 Year

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

SECTION 4

Testing Matrices



PRESCIENT

ASSURANCE

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

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

Prescient Assurance LLC conducted the examination testing throughout the period February 27, 2024 to May 27, 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: 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.

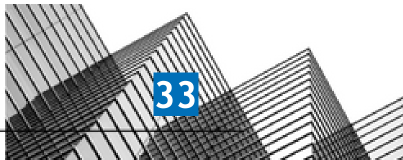
Trust ID	COSO Principle	Control Description	Test Applied by the Service Auditor	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.	Inspected the Human Resource Security Policy to determine that the company performs background checks on new employees. Observed background checks for all 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.	Observed a sample of the eligible population of contractor agreements for the onboarded contractors to determine that they include a relevant code of conduct section.	No exceptions noted.
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.	Observed the employee acceptance document to determine that all employees acknowledge the code of conduct at the time of hire. Additionally, inquired with the company which states that there were no code of conduct violations during the audit period and no employee was subject to disciplinary actions during the 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 service agreements for sample contractors engaged with during the audit period to determine that contractors are required to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to sign a confidentiality	Inspected agreements signed by an employee hired during the audit period to determine that employees are required to sign a confidentiality agreement during onboarding.	No exceptions noted.

		agreement during onboarding.		
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 the Performance Review of an employee 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.	Inspected the Board of Directors meeting minutes dated May 1, 2024, to determine that the company's Board of Directors meets at least annually and maintains formal meeting minutes	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 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 LinkedIn profiles of the board members, 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. Additionally, observed the meeting minutes to determine that the board engages third-party information security experts and consultants 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 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 Board of Directors meeting minutes dated May 1, 2024, documenting discussions of the company's state of cybersecurity to determine that the company's board of directors meets at least annually to discuss the state of the company's cybersecurity and privacy risk.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate	The company management has established	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of the IT	No exceptions noted.

	authorities and responsibilities in the pursuit of objectives.	defined roles and responsibilities to oversee the design and implementation of information security controls.	Manager for the design, development, implementation, and monitoring of security controls have been defined.	
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 of the company showing the reporting lines and positions of authority to determine that the company has a formal organizational chart in place that is accessible to internal personnel.	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 VP of Engineering for the design, development, implementation, and monitoring of security controls have been defined.	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 the Performance Review of an employee 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 Human Resource Security Policy to determine that the company performs background checks on new employees. Observed background checks for all 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,	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of the VP of Engineering for the design, development, implementation, and	No exceptions noted.

		operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	monitoring of security controls have been defined.	
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 security awareness training completion record to determine that the company requires employees to complete security awareness training at the time of hire and annually thereafter.	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.	Observed the employee acceptance document to determine that all employees acknowledge the code of conduct at the time of hire. Additionally, inquired with the company which states that there were no code of conduct violations during the audit period and no employee was subject to disciplinary actions during the 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 VP of Engineering for the design, development, implementation, and monitoring of security controls have been defined.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal	The company managers are	Inspected the Performance Review of an employee to determine that the	No exceptions noted.

	control responsibilities in the pursuit of objectives.	required to complete performance evaluations for direct reports at least annually.	company managers are required to complete performance evaluations for direct reports at least annually.	
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 the Papertrail log management and message API code to determine that the company has a log management tool in place to identify events that may have a potential impact on the company's ability to achieve its security objectives.	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 remediated vulnerabilities to determine that the company uses GitHub, configured on Vanta, to perform host-based vulnerability scans on all external-facing systems and that critical and high vulnerabilities are remediated within SLAs.	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.	Observed that the company uses Vanta for continuous self-assessment and monitoring of internal controls.	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 requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the security awareness training completion record to determine that the company requires employees to complete security awareness training at the time of hire and annually thereafter.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support	The company has established a formalized whistleblower policy, and an	Inspected the company's Whistleblower Form to determine that the company has an anonymous communication channel in place for users to report potential issues or fraud concerns.	No exceptions noted.



	the functioning of internal control.	anonymous communication channel is in place for users to report potential issues or fraud concerns.		
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 internal users.	Inspected the Slack channel displaying product updates to determine that the company communicates system changes to authorized internal 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.	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 VP of Engineering 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 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 company's website and Customer Onboarding training presentation to determine that the company provides a description of its products and services 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 IT Manager 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 control, necessary to support	The company's information security policies and procedures are documented	Inspected the Access Control Policy, Incident Response Plan, Information Security Policy, and other policies have been reviewed in 2024 to determine that the company has established information	No exceptions noted.

	the functioning of internal control.	and reviewed at least annually.	security policies and reviews them annually.	
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.	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 company's website and Customer Onboarding training presentation to determine that the company provides a description of its products and services 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 Customer Onboarding Training presentation slides 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 dashboard displaying the admin email to determine that the company has an external-facing support system in place that allows users to report concerns.	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 Terms of Services for sample vendors to determine that the agreements include confidentiality and privacy commitments applicable to the entity.	No exceptions noted.

CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company notifies customers of critical system changes that may affect their processing.	Inspected client email communication to customer regarding a new feature to determine that customers are notified of critical system changes that may affect their processing.	No exceptions noted.
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 Service to determine that service and privacy commitments are communicated to customers through official documents.	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 company requires a risk register to be maintained, risks to be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its 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 risk management processes along with risk response and treatment strategies have been documented that help the company achieve its business objectives. Inspected the risk assessment data to determine that the company conducts risk assessments to protect its financial and production data.	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	Inspected the Risk Management Policy to determine that the company requires a risk register to be maintained, risks to be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its risk management program.	No exceptions noted.

		threats, and mitigation strategies for those risks.		
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 the company's Disaster Recovery test exercise report dated May 30, 2024, to determine that the company tests its BC/DR plan at least annually.	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 the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment data completed within the observation period to determine that the company conducts risk assessments to protect its financial and production data at least annually.	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 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 vendor inventory on the compliance management platform to determine that the company maintains a list of vendors, their risk levels, and links to their security and privacy commitments. Moreover, it is noted there are no high risk vendors. Inspected the security certificates reviewed in March 2024 to determine that the company completes reviews of critical third-party vendors at least annually.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing	The company's risk assessments are	Inspected the risk assessment data completed within the observation period	No exceptions noted.

	risks to the achievement of objectives.	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.	to determine that the company conducts risk assessments to protect its financial and production data at least annually.	
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 company requires a risk register to be maintained, risks to be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its 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 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	Inspected the risk assessment data completed within the observation period to determine that the company conducts risk assessments to protect its financial and production data at least annually.	No exceptions noted.

		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 the snapshot of GitHub dashboard displaying build configurations and status to determine that a CI/CD system is in use and that changes are documented and deployed consistently.	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 company requires a risk register to be maintained, risks to be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its 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 vendor inventory on the compliance management platform to determine that the company maintains a list of vendors, their risk levels, and links to their security and privacy commitments. Moreover, it is noted that there are no high risk vendors. Inspected the security certificates reviewed in March 2024 to determine that the company completes reviews of critical third-party vendors at least annually.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the	The company performs control self-assessments at least annually	Observed that the company uses Vanta for continuous self-assessment and monitoring of internal controls.	No exceptions noted.

	components of internal control are present and functioning.	to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.		
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 remediated vulnerabilities to determine that the company uses GitHub, configured on Vanta, to perform host-based vulnerability scans on all external-facing systems and that critical and high vulnerabilities are remediated within SLAs.	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 vendor inventory on the compliance management platform to determine that the company maintains a list of vendors, their risk levels, and links to their security and privacy commitments. Moreover, it is noted that there are no high risk vendors. Inspected the security certificates reviewed in March 2024 to determine that the company completes reviews of critical third-party vendors at least annually.	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.	Observed that the company uses Vanta for continuous self-assessment and monitoring of internal controls.	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	Inspected the Access Control Policy, Incident Response Plan, Information Security Policy, and other policies have been reviewed in 2024 to determine that the company has established information	No exceptions noted.

		and reviewed at least annually.	security policies and reviews them annually.	
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 mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the company requires a risk register to be maintained, risks to be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its risk management program.	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 information security policies and procedures are documented and reviewed at least annually.	Inspected the Access Control Policy, Incident Response Plan, Information Security Policy, and other policies have been reviewed in 2024 to determine that the company has established information security policies and reviews them annually.	No exceptions noted.
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	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.

		existing user's access.		
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 Data Management Policy to determine that internal data retention and disposal procedures have been established stating that the company is obliged to ensure that the information is destroyed following the rules defined for their level of classification.	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 backups 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 the branch protection rule in Github and sample changes pushed to production during the audit period to determine that changes are required to be 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	The company's information security policies	Inspected the Access Control Policy, Incident Response Plan, Information Security Policy, and other policies have	No exceptions noted.

	in procedures that put policies into action.	and procedures are documented and reviewed at least annually.	been reviewed in 2024 to determine that the company has established information security policies and reviews them annually.	
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 VP of Engineering for the design, development, implementation, and monitoring of security controls have been defined.	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 vendor inventory on the compliance management platform to determine that the company maintains a list of vendors, their risk levels, and links to their security and privacy commitments. Moreover, it is noted that there are no high risk vendors. Inspected the security certificates reviewed in March 2024 to determine that the company completes reviews of critical third-party vendors at least 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 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.	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 specifies its objectives to enable the identification and assessment of risk	Inspected the Risk Management Policy to determine that the risk management processes along with risk response and treatment strategies have been documented that help the company achieve its business objectives.	No exceptions noted.

		related to the objectives.	Inspected the risk assessment data to determine that the company conducts risk assessments to protect its financial and production data.	
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 company requires a risk register to be maintained, risks to be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its 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 keys.	Inspected the list of users having access to Heroku and GitHub to determine that the employees having access to datastores have MFA enabled.	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 list of users with access to Heroku to determine that privileged access to encryption keys is restricted to authorized users.	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.		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.	Observed that the entity does not manage employee computers' operating system but uses Vanta as an MDM agent.	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 list of users with access to Heroku to determine that privileged access to the production network is restricted to authorized users.	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 tickets for access requested during the audit period to determine that access to systems requires documented access request and approval prior to 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 requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the list of users having access to in-scope systems and applications along with their unique User IDs and MFA configurations and status to determine that the company has an authentication mechanism in place.	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 password configurations and multifactor authentication enablement for in-scope systems to determine that the passwords are 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 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 possessing a valid multi-factor authentication (MFA) method.	Inspected password configurations for in-scope systems to determine that production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	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 datastores housing sensitive customer data are encrypted at rest.	Inspected Postgresql database record and encryption status to determine that user data is 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 Data Management Policy to determine that the company has established a data classification scheme and handling procedures for confidential, public, and restricted 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 restricts access to migrate changes to production to authorized personnel.	Inspected the list of users having authorization to migrate code changes into production 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 including the Heroku database, employee computers, and GitHub repository to determine that the company maintains a formal inventory of 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 list of users having access to Heroku along with MFA configurations to determine that the users having access to the production network have unique user IDs and MFA-enabled.	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 list of users with access to Spara console to determine that privileged access to the application is restricted to authorized users.	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 databases to authorized users with a business need.	Observed that the company uses Heroku databases as a production database. Inspected list of users having privileged access to Heroku to determine that the company restricts privileged access to databases to authorized users	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 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 July 20, 2024, 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 access review report to determine that the company performs access review at least quarterly.	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 when user access is no longer authorized.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Confirmed with the entity that there were no employees terminated during the audit period.	Not tested. No employees were terminated during the review period.
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 list of users having access to Heroku along with MFA configurations to determine that the users having access to the production network have unique user IDs and MFA-enabled.	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 tickets for access requested during the audit period to determine that access to systems requires documented access request and approval prior to 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 list of users having access to Heroku along with MFA configurations to determine that the users having access to the production network have unique user IDs and MFA-enabled.	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	The company completes termination checklists to ensure that access is revoked for terminated	Confirmed with the entity that there were no employees terminated during the audit period.	Not tested. No employees were terminated during the review period.

	and segregation of duties, to meet the entity's objectives.	employees within SLAs.		
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 access review report to determine that the company performs access review at least quarterly.	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 tickets for access requested during the audit period to determine that access to systems requires documented access request and approval prior to 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	Inspected the access review report to determine that the company performs access review at least quarterly.	No exceptions noted.

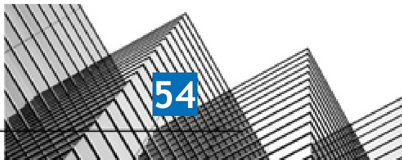
		are tracked to completion.		
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Confirmed with the entity that there were no employees terminated during the audit period.	Not tested. No employees were terminated during the review period.
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 Data Management Policy to determine that internal data retention and disposal procedures have been established stating that the company is obliged to ensure that the information is destroyed following the rules defined for their level of classification.	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.	Confirmed that no data deletion request was received within the audit period.	Not tested. No data deletions were initiated during the review period.
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 July 20, 2024, 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 list of users having access to Heroku along with MFA configurations to determine that the users having access to the production network have unique user IDs and MFA-enabled.	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.	Observed that user activity and API use is tracked by Heroku and regions and employees' computers are monitored with Vanta. Inspected the Cloudflare WAF to determine that the company uses 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 firewall ruleset review report dated March 22, 2024, to determine that the company reviews its firewall rulesets at least annually.	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 Cloudflare WAF to determine that the company uses firewall features of AWS and configures them 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 the record of remediated vulnerabilities to determine that the company applies patches to infrastructure as part of routine maintenance.	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 Operations Security Policy to determine that systems and networks are required to be provisioned and maintained in accordance with the configuration and hardening standards. Observed that the company uses Heroku and Cloudflare as its cloud infrastructure provider which maintains industry-level network and system hardening standards.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from	The company uses secure data transmission	Inspected the security certificate on the company's website which is valid until July 20, 2024, and the company website	No exceptions noted.

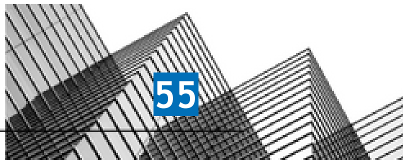
	sources outside its system boundaries.	protocols to encrypt confidential and sensitive data when transmitted over public networks.	redirects HTTP to HTTPS via a 3XX status code, to determine that the company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	
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 password configurations for in-scope systems to determine that 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 on the company's website which is valid until July 20, 2024, and the company website redirects HTTP to HTTPS via a 3XX status code, to determine that the company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	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 has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected Computer Directory on Vanta to determine that the company uses Vanta as an MDM.	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 the record of remediated vulnerabilities to determine that the company applies patches to infrastructure as part of routine maintenance.	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 the antivirus software installation record of employee workstations to determine that the company employees 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 the snapshot of GitHub dashboard displaying build configurations and status to determine that a CI/CD system is in use and that changes are documented and deployed consistently.	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 remediated vulnerabilities to determine that the company uses GitHub, configured on Vanta, to perform host-based vulnerability scans on all external-facing systems and that critical and high vulnerabilities are remediated within SLAs.	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	The company's risk assessments are performed at least annually. As part of this process,	Inspected the risk assessment data completed within the observation period to determine that the company conducts risk assessments to protect its financial and production data at least annually.	No exceptions noted.

	introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	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.		
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 the branch protection rule in Github and sample changes pushed to production during the audit period to determine that changes are required to be 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 Operation Security Policy to determine that vulnerability management and system monitoring procedures have been documented by the company with the Engineering departments being primarily 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	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are	Inspected the remediated vulnerabilities to determine that the company uses GitHub, configured on Vanta, to perform host-based vulnerability scans on all external-facing systems and that critical and high vulnerabilities are remediated within SLAs.	No exceptions noted.



	analyzed to determine whether they represent security events.	tracked to remediation.		
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.	Observed that user activity and API use is tracked by Heroku and regions and employees' computers are monitored with Vanta. Inspected the Cloudflare WAF to determine that the company uses 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 the Papertrail, Heroku performance monitoring configurations, and alert configurations to determine that the company has an infrastructure monitoring tool utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	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 the Papertrail log management and message API code to determine that the company has a log management tool in place to identify events that may have a potential impact on the company's ability to achieve its security objectives.	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 Operation Security Policy to determine that vulnerability management and system monitoring procedures have been documented by the company with the Engineering departments being primarily 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	The company has infrastructure supporting the service patched as a part of routine	Inspected the record of remediated vulnerabilities to determine that the company applies patches to infrastructure as part of routine maintenance.	No exceptions noted.



	disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.		
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.	Confirmed with the entity that there were no security and privacy incidents that occurred during the audit period.	Not tested. No security and privacy incidents were detected during the review period.
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.	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 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 record of remediated vulnerabilities to determine that the company applies patches to infrastructure as part of routine maintenance.	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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high	Inspected the remediated vulnerabilities to determine that the company uses GitHub, configured on Vanta, to perform host-based vulnerability scans on all external-facing systems and that critical and high vulnerabilities are remediated within SLAs.	No exceptions noted.

		vulnerabilities are tracked to remediation.		
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.	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.	Observed an incident response plan report from May 3, 2024 to determine that the company tests their 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.	Confirmed with the entity that there were no security and privacy incidents that occurred during the audit period.	Not tested. No security and privacy incidents were detected during the review period.
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.	Observed an incident response plan report from May 3, 2024 to determine that the company tests their incident response plan at least annually.	No exceptions noted.
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.	Confirmed with the entity that there were no security and privacy incidents that occurred during the audit period.	Not tested. No security and privacy incidents were detected during the review period.

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.	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 the company's Disaster Recovery test exercise report dated May 30, 2024, to determine that the company tests its BC/DR plan at least annually.	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 the branch protection rule in Github and sample changes pushed to production during the audit period to determine that changes are required to be 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 the record of remediated vulnerabilities to determine that the company applies patches to infrastructure as part of routine maintenance.	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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are	Inspected the remediated vulnerabilities to determine that the company uses GitHub, configured on Vanta, to perform host-based vulnerability scans on all external-facing systems and that critical and high vulnerabilities are remediated within SLAs.	No exceptions noted.

		tracked to remediation.		
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 list of users having authorization to migrate code changes into production 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 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 Operations Security Policy to determine that systems and networks are required to be provisioned and maintained in accordance with the configuration and hardening standards. Observed that the company uses Heroku and Cloudflare as its cloud infrastructure provider which maintains industry-level network and system hardening standards.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	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 company requires a risk register to be maintained, risks to be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its risk management program.	No exceptions noted.

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 data completed within the observation period to determine that the company conducts risk assessments to protect its financial and production data at least annually.	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.
CC9.2	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 Terms of Services for sample vendors to determine that the agreements include confidentiality and privacy commitments applicable to the entity.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management	Inspected the vendor inventory on the compliance management platform to determine that the company maintains a	No exceptions noted.

		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.	list of vendors, their risk levels, and links to their security and privacy commitments. Moreover, it is noted that there are no high risk vendors. Inspected the security certificates reviewed in March 2024 to determine that the company completes reviews of critical third-party vendors at least annually.	