Insight Assurance

Delivering Quality, Assuring Trust.

System and Organization Controls Report (SOC 2® Type 2)

Report on RubyWell, Inc.'s Description of Its RubyWell Platform and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Throughout the Period October 1, 2024, to December 31, 2024

RubyWell

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT

Insight Assurance
Delivering Quality, Assuring Trust.

INDEPENDENT SERVICE AUDITOR'S REPORT

To: RubyWell, Inc.

Scope

We have examined RubyWell, Inc.'s ("RubyWell" or "the Service Organization") description of its RubyWell Platform found in Section 3 titled "RubyWell, Inc.'s description of its RubyWell Platform" throughout the period October 1, 2024, to December 31, 2024 ("description") based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2024, to December 31, 2024, to provide reasonable assurance that RubyWell's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria*.

RubyWell uses Amazon Web Services (AWS) to provide hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at RubyWell, to achieve RubyWell's service commitments and system requirements based on the applicable trust services criteria. The description presents RubyWell's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of RubyWell'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 RubyWell, to achieve RubyWell's service commitments and system requirements based on the applicable trust services criteria. The description presents RubyWell's controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of RubyWell's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The information included in Section 5 "Other Information Provided by RubyWell, Inc. is presented by management of RubyWell to provide additional information and is not part of RubyWell, Inc.'s description. Information about RubyWell management responses to exceptions has not been subjected to the procedures applied in the examination of the description and the suitability of the design and operating effectiveness of controls to meet the applicable trust services criteria, and accordingly, we do not express an opinion on it.

Service Organization's Responsibilities

RubyWell is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that RubyWell's service commitments and system requirements were achieved. In Section 2, RubyWell has provided the accompanying assertion titled "RubyWell, Inc.'s Management Assertion" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. RubyWell is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria, and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

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

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

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

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

Inherent Limitations

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

Emphasis of Matter – Controls Did Not Operate During the Period Covered by the Report

The Service Organization's description of its RubyWell Platform discusses its policies and procedures to require changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment. However, during the period from October 1, 2024, to December 31, 2024, the Service Organization had no code, system, or infrastructure changes that would warrant the operation of the controls stated above. Because these controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using the following trust services criteria:

- 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 Service Organization's description of its RubyWell Platform discusses its security incident response and recovery plan, which includes the controls implemented and operated to respond to and recover from security incidents. However, during the period October 1, 2024, to December 31, 2024, the Service Organization did not experience a security incident that would warrant the operation of the response and recovery processes and controls within its security incident response and recovery plan. Because those controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using the following trust services criteria:

- CC7.4, *The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.*
- CC7.5, *The entity identifies, develops, and implements activities to recover from identified security incidents.*

Our opinion is not modified with respect to the matters emphasized.

Description of Test of Controls

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

Opinion

In our opinion, in all material respects,

- the description presents RubyWell's Platform that was designed and implemented throughout the period October 1, 2024, to December 31, 2024, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period October 1, 2024, to December 31, 2024, to provide reasonable assurance that RubyWell's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of RubyWell's controls throughout that period.
- the controls stated in the description operated effectively throughout the period October 1, 2024, to December 31, 2024, to provide reasonable assurance that RubyWell's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and user entity controls assumed in the design of RubyWell's controls operated effectively throughout that period.

Restricted Use

This report is intended solely for the information and use of RubyWell, user entities of RubyWell's RubyWell Platform throughout the period October 1, 2024, to December 31, 2024, and business partners of RubyWell subject to risks arising from interactions with the RubyWell Platform, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Insight Assurance LLC

Tampa, Florida
April 2, 2025

SECTION 2: RUBYWELL, INC.'S MANAGEMENT ASSERTION

RubyWell

RUBYWELL, INC.'S MANAGEMENT ASSERTION

We have prepared the description of RubyWell, Inc.'s ("RubyWell" or "the Service Organization") RubyWell Platform entitled "RubyWell, Inc.'s description of its RubyWell Platform" throughout the period October 1, 2024, to December 31, 2024 ("description") based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria) The description is intended to provide report users with information about the RubyWell Platform that may be useful when assessing the risks arising from interactions with RubyWell's system, particularly information about system controls that RubyWell has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

RubyWell uses Amazon Web Services (AWS) to provide hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at RubyWell, to achieve RubyWell's service commitments and system requirements based on the applicable trust services criteria. The description presents RubyWell's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of RubyWell'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 RubyWell, to achieve RubyWell's service commitments and system requirements based on the applicable trust services criteria. The description presents the subservice organization controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of RubyWell's controls.

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

- the description presents RubyWell's Platform that was designed and implemented throughout the period October 1, 2024, to December 31, 2024, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period October 1, 2024, to December 31, 2024, to provide reasonable assurance that RubyWell's service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organization and user entities applied the complementary controls assumed in the design of RubyWell's controls.

- the controls stated in the description operated effectively throughout the period October 1, 2024, to December 31, 2024, to provide reasonable assurance that RubyWell's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of RubyWell's controls operated effectively throughout that period.

RubyWell, Inc.
April 2, 2025

SECTION 3: RUBYWELL, INC.'S DESCRIPTION OF ITS RUBYWELL PLATFORM

RUBYWELL, INC.'S DESCRIPTION OF ITS RUBYWELL PLATFORM

COMPANY BACKGROUND

RubyWell, Inc. ("RubyWell") is a privately held company established on September 25th, 2024, offers services to family caregivers and their care recipients. RubyWell is a DE Corporation headquartered in New York, New York.

DESCRIPTION OF SERVICES OVERVIEW

RubyWell is a technology company using RubyWell Platform that helps patients, caregivers, and care teams work together to safely manage health at home.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

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

Security Commitments

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

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

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

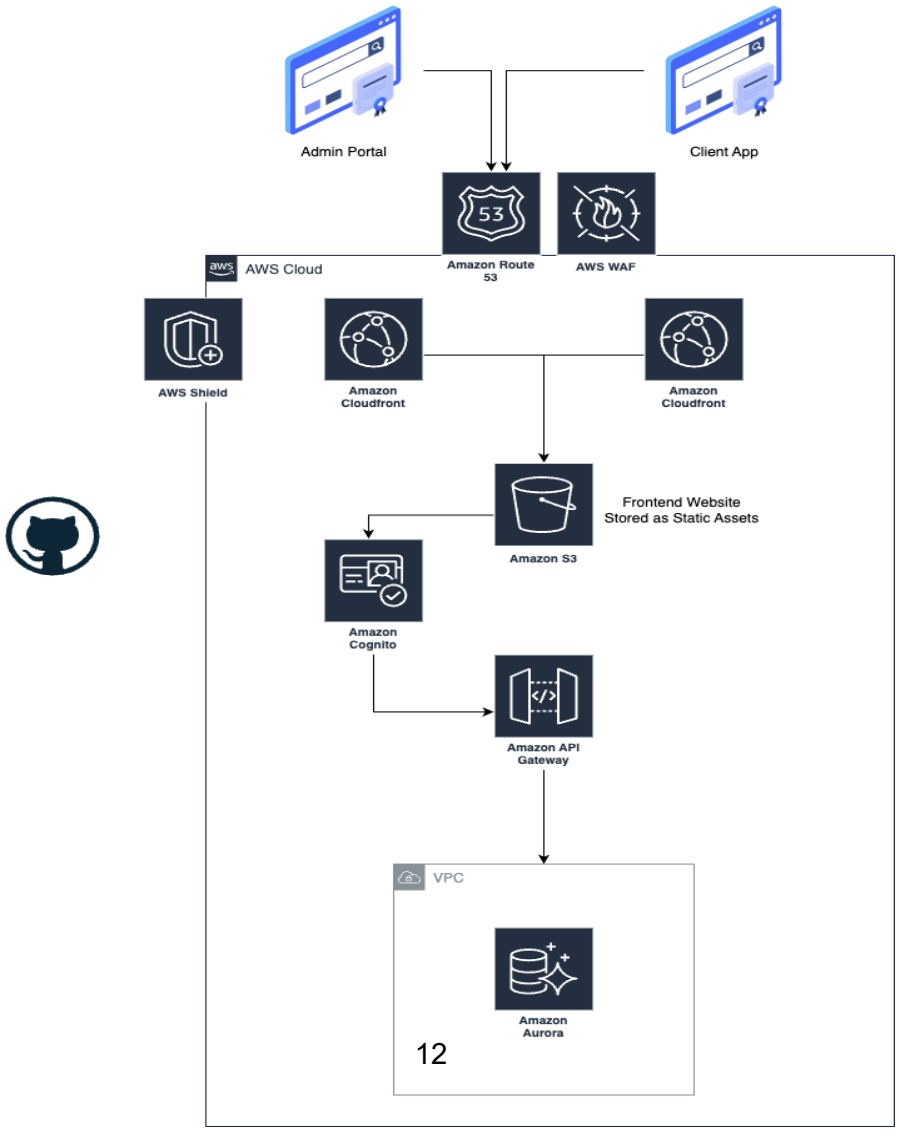
The System description is comprised of the following components:

- **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.

INFRASTRUCTURE

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



Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS Elastic Compute Cloud (EC2)	AWS	Provides secure, resizable compute capacity in the cloud to deploy the service
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage, upload, and download

SOFTWARE

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

Primary Software		
System/Application	**Operating System**	**Purpose**
GuardDuty	AWS	Security application used for automated intrusion detection (IDS)
Datadog	Datadot	Monitoring application used to provide monitoring, alter, and notification services for RubyWell platform
GitHub	GitHub	Code repository platform used for version control and developer collaboration
Google Workspace	Google Workspace	Productivity suite used to create, store, and collaborate on documents, emails, and meetings
Linear	Linear	Project management tool used for issue tracking and product development workflows
Segment	Segment	Customer data platform used to collect and route user information across marketing and analytics tools
Sentry	Sentry	Application Performance Monitoring & Error Tracking
Slack	Slack	Team communication and collaboration platform
Typeform	Typeform	Form building solution
Vanta	Vanta	Compliance automation tool used to prepare for security certifications and monitor regulatory requirements

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.

RubyWell has a staff of approximately ten (10) organized in the following functional areas:

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

This includes:

Chief Executive Officer (CEO) – Responsible for the mission, vision, execution and compliance of the company

Chief Finance Officer (CFO) – Responsible for the financial strategy, financial reporting, and financial compliance of the company

Director of Engineering – Responsible for engineering architecture, code design and integrity, and security.

Chief Product Officer (CPO) – Responsible for product design, product compliance, and product innovation for the company

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

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

Product Development – Responsible for the development, testing, and maintenance of the product. Responsible for the product life cycle, including adding additional product functionality.

DATA

Data as defined by RubyWell, constitutes the following:

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

Data is categorized in the following major types of data used by RubyWell.

Data		
Category	**Description**	**Examples**
Public	Public information is not confidential and can be made public without any implications for RubyWell.	• 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 RubyWell. RubyWell 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 RubyWell to operate the business. RubyWell 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 personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, RubyWell has policies and procedures in place to ensure proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

PROCEDURES

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

- Physical Security
- Logical Access

- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security

RubyWell's production servers are maintained by AWS. Physical and environmental security protection are the responsibility of AWS. RubyWell reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

Logical Access

RubyWell provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privileged access to identified users and to maintain simple and reportable user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are reviewed on a quarterly basis to ensure the least privileged access.

The onboarding Team 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 RubyWell's policies and completing security training. These steps must be completed within fourteen (14) days of hire.

When an employee is terminated, the offboarding Team is responsible for deprovisioning access to all in scope systems for that employee's termination.

Change Management

RubyWell 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.

Patch Management

Software patches and updates are applied to systems in a timely manner. Infrastructure supporting the services provided is patched as a part of the change management process to help ensure that servers supporting the service are hardened against security threats. Routine updates are applied after thorough testing. In the case of updates to correct known vulnerabilities, priority will be given to testing to speed the time to production. Critical security patches are applied within three days from identification and non-critical security patches are applied within seven days after identification.

Backups and Recovery

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

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

Computer Operations

RubyWell 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.

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

RubyWell 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.

Problem Management

RubyWell maintains an Incident Response Policy that describes the process for identifying and addressing potential security incidents. The policy details exactly what must occur if an incident is suspected and covers both electronic and physical security incidents. Plans for detecting, responding to, and recovering from incidents are included in the policy, and post-incident activity requirements are defined. To ensure responsible employees are prepared to respond to incidents, the organization provides formal security breach training.

RubyWell provides a customer service request form where clients can report potential security breaches, and clients are also provided with an email and phone number for the same purpose. Internal users are directed to report incidents through an internal portal for documentation and tracking purposes.

Data Communications

RubyWell 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

RubyWell 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.

System Monitoring

The Operations Security Policy describes the organization's policies and procedures related to network logging and monitoring as well as vulnerability identification and remediation. The organization uses AWS VPC logs, S3 Server logs and CloudTrail for system logging within the AWS environment, and the organization collects logs from the firewall. AWS VPC logs, S3 Server logs and CloudTrail and firewall logs document source IP, destination IP, destination port, protocol type, and timestamp. The organization monitors system capacity using CloudWatch Alarms.

AWS GuardDuty is used for threat detection purposes, and the tool generates logs, VPC flow logs, and DNS logs for intrusion detection.

The vulnerability assessment process involves the execution of CIS testing, implementation of antivirus software, and system patching. The organization uses Xprotect anti-malware and has configured the software to run updates daily and prohibit end-users from disabling or altering the software. Alerts are sent immediately when a potential virus is detected, and logs are generated and retained for at least one year with at least three months readily available. Vulnerability Scanning is used to identify newly emerging vulnerabilities, and the organization monitors vendors, for patch updates to correct vulnerabilities.

Vendor Management

The organization maintains a Third-Party Management Policy that includes requirements for interacting with vendors/service providers. The policy includes requirements for performing due diligence measures prior to engaging with a new provider. Due diligence procedures include evaluating each material IT vendors' cost-effectiveness, functionality/services, risk, financial viability, compliance, and performance. The organization is required to define service levels when negotiating an arrangement with a new vendor or re-negotiating an existing arrangement, and all service levels are agreed upon and documented clearly. The organization monitors its providers' service levels to ensure each provider is providing the agreed-upon services and is compliant with all requirements. The organization executes non-disclosure agreements with third parties before any information is shared.

Boundaries of the System

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

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

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

CONTROL ENVIRONMENT

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across an organization. The organizational structure, separation of job responsibilities by departments and business function, documentation of policies and procedures, and internal audits are the methods used to define, implement and ensure effective operational controls. The Board of Directors and/or senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct.

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

Management Philosophy and Operating Style

The RubyWell 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 RubyWell 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 RubyWell 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.

Commitment to Competence

RubyWell'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.

Organizational Structure and Assignment of Authority and Responsibilities

RubyWell'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.

RubyWell'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.

Human Resources Policies and Procedures

RubyWell'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. RubyWell'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 acknowledegment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Personnel termination procedures are in place to guide the termination process and are documented in a termination checklist.

RISK ASSESSMENT PROCESS

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

Integration with Risk Assessment

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

CONTROL ACTIVITIES

Control activities are the actions established by policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are executed. Control activities are performed at all levels of the organization and various stages within business processes, and over the technology environment.

INFORMATION AND COMMUNICATION SYSTEMS

Information and communication are an integral component of RubyWell’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.

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

MONITORING CONTROLS

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. RubyWell’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 are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

Ongoing Monitoring

RubyWell’s management conducts quality assurance monitoring on a continuous 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 RubyWell’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 to address 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 RubyWell’s personnel.

Monitoring of the Subservice Organization

RubyWell uses a subservice organization to provide hosting services.

The management of RubyWell receives and reviews the SOC 2 report of the AWS on an annual basis. In addition, through its daily operational activities, the management of RubyWell monitors the services performed by AWS to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively.

Reporting Deficiencies

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

CHANGES TO THE SYSTEM DURING THE PERIOD

No significant changes have occurred to the services provided to user entities during the examination period.

SYSTEM INCIDENTS DURING THE PERIOD

No significant incidents have occurred to the service provided to user entities during the examination period.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

RubyWell's controls related to the System cover only a portion of overall internal control for each user entity of RubyWell. It is not feasible for the trust services criteria related to the System to be achieved solely by RubyWell. Therefore, each user entity's internal controls should be evaluated in conjunction with RubyWell's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

#	Complementary Subservice Organization Controls (CSOC)	Related Criteria
1	AWS is responsible for maintaining physical security and environmental protection controls over the data centers hosting the RubyWell infrastructure.	CC6.4
2	AWS is responsible for the destruction of physical assets hosting the production environment.	CC6.5

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

RubyWell'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 RubyWell's services to be solely achieved by RubyWell control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of RubyWell's.

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

1. User entities are responsible for understanding and complying with their contractual obligations to RubyWell.
2. User entities are responsible for notifying RubyWell of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring supervision, management, and control of the use of RubyWell services by their personnel.

5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize RubyWell services.
6. User entities are responsible for providing RubyWell with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying RubyWell of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

TRUST SERVICES CATEGORY CRITERIA, AND RELATED CONTROLS

The Security category and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. The criteria and controls designed, implemented, and operated to meet them ensure that information, systems, and access (physical and logical) are protected against unauthorized access, and systems are available for operation and use. The controls supporting the applicable trust services criteria are included in Section 4 of this report and are an integral part of the description of the system.

For specific criteria, which were deemed not relevant to the system, see Section 4 for the related explanation.

SECTION 4: TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS AND TESTS OF CONTROLS

Trust Services Category Criteria, Related Controls, and Tests of Controls

This SOC 2 Type 2 report was prepared in accordance with the AICPA attestation standards and has been performed to examine the suitability of the design and operating effectiveness of controls to meet the criteria for the Security category set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria* throughout the period October 1, 2024, to December 31, 2024.

The applicable trust services criteria and related controls specified by RubyWell are presented in Section 4 of this report.

Test procedures performed in connection with determining the operating effectiveness of controls detailed here in Section 4 are described below:

- Inquiries – Inquiry of appropriate personnel and corroboration with management.
- Observation – Observation of the application, performance, or existence of the control.
- Inspection – Inspection of documents and reports indicating the performance of the control.
- Reperformance – Reperformance of the control.

Footnotes for Test Results When No Tests of Operating Effectiveness Were Performed

1. The circumstances that warranted the operation of the control did not occur during the examination period; therefore, no tests of operating effectiveness were performed.
2. The operation of the periodic control was performed prior to the examination period; therefore, no tests of operating effectiveness were performed.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.1 – COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The company has an approved Code of Conduct that is reviewed annually and updated as needed. Sanction policies are documented within the information security policies and procedures.	Inspected the company's Code of Conduct Policy to determine that Code of Conduct was in place.	No exceptions noted.
		Per inquiry with management and inspection of company's compliance platform, the Code of Conduct was last reviewed in September 2024; therefore, no testing was performed.	No testing performed.[2]
		Inspected the company's information security policies and procedures to determine that sanction policies were documented within the information security policies and procedures.	No exceptions noted.
CC1.1.2	The company requires new employees and contractors to acknowledge the Code of Conduct at the time of hire and communicates the Code of Conduct continuously to active employees and contractors through the compliance tool.	Inspected the Code of Conduct acknowledgment for a sample of new contractors to determine that the Code of Conduct was acknowledged at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's personnel listing, there were no newly hired employees during the examination period; therefore, no testing was performed.	No testing performed.[1]
		Inspected the compliance tool and determined the Code of Conduct is communicated continuously to active employees and contractors through the compliance tool.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.1.3	The company requires new employees and contractors to review and acknowledge the information security policies at the time of hire and communicates the information security policies continuously to active employees and contractors through the compliance tool.	Inspected the information security policies acknowledgment for a sample of contractors to determine that the information security policies were acknowledged at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's personnel listing, there were no newly hired employees during the examination period; therefore, no testing was performed.	No testing performed.[1]
		Inspected the compliance tool and determined the information security policies are communicated continuously to active employees and contractors through the compliance tool.	No exceptions noted.
CC1.1.4	The company's managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of active employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.
CC1.1.5	The company performs background checks on new employees and contractors.	Inspected the completed background check for a sample of contractors to determine whether the company performed background checks on contractors.	No exceptions noted.
		Per inquiry with management and inspection of the company's personnel listing, there were no newly hired employees during the examination period; therefore, no testing was performed.	No testing performed.[1]

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.1.6	Employees and contractors are required to review and acknowledge the confidentiality agreement at the time of hire.	Inspected the signed contractor agreements for a sample of contractors to determine that contractors were required to review and acknowledge the confidentiality agreement at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's personnel listing, there were no newly hired employees during the examination period; therefore, no testing was performed.	No testing performed.[1]
CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
RubyWell does not have any independent board of directors; therefore, this criterion is not applicable.			
CC1.3 – COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the company's organizational chart to determine that the company maintained an organizational chart that described the organizational structure and reporting lines.	No exceptions noted.
CC1.3.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	Inspected the company's Information Security Roles and Responsibilities Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.3.3	The company requires new employees and contractors to review and acknowledge the information security policies at the time of hire and communicates the information security policies continuously to active employees and contractors through the compliance tool.	Inspected the information security policies acknowledgment for a sample of contractors to determine that the information security policies were acknowledged at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's personnel listing, there were no newly hired employees during the examination period; therefore, no testing was performed.	No testing performed.[1]
		Inspected the compliance tool and determined the information security policies are communicated continuously to active employees and contractors through the compliance tool.	No exceptions noted.
CC1.4 – COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	The company performs background checks on new employees and contractors.	Inspected the completed background check for a sample of contractors to determine whether the company performed background checks on contractors.	No exceptions noted.
		Per inquiry with management and inspection of the company's personnel listing, there were no newly hired employees during the examination period; therefore, no testing was performed.	No testing performed.[1]

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.4.2	The company's managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of active employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.
CC1.4.3	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	Inspected the company's Information Security Roles and Responsibilities Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned.	No exceptions noted.
CC1.4.4	The company requires new employees and contractors to complete security awareness training at the time of hire and active employees and contractors to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Inspected the training records for a sample of contractors to determine that the company required contractors to complete security awareness training at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's personnel listing, there were no newly hired employees during the examination period; therefore, no testing was performed.	No testing performed.[1]

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.4.4 (*cont.*)	The company requires new employees and contractors to complete security awareness training at the time of hire and active employees and contractors to complete security training at least annually.	Per inquiry with management and inspection of company's compliance tool, the annual security awareness training for active employees and contractors was completed in September 2024; therefore, no testing was performed.	No testing performed.[2]
CC1.5 – COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	The company has an approved Code of Conduct that is reviewed annually and updated as needed. Sanction policies are documented within the information security policies and procedures.	Inspected the company's Code of Conduct Policy to determine Code of Conduct was in place.	No exceptions noted.
		Per inquiry with management and inspection of company's compliance platform, the Code of Conduct was last reviewed in September 2024; therefore, no testing was performed.	No testing performed.[2]
		Inspected the company's information security policies and procedures to determine that sanction policies were documented within the information security policies and procedures.	No exceptions noted.
CC1.5.2	The company requires new employees and contractors to acknowledge the Code of Conduct at the time of hire and communicates the Code of Conduct continuously to active employees and contractors through the compliance tool.	Inspected the Code of Conduct acknowledgment for a sample of new contractors to determine that the Code of Conduct was acknowledged at the time of hire.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.5.2 (*cont.*)	The company requires new employees and contractors to acknowledge the Code of Conduct at the time of hire and communicates the Code of Conduct continuously to active employees and contractors through the compliance tool.	Per inquiry with management and inspection of the company's personnel listing, there were no newly hired employees during the examination period; therefore, no testing was performed.	No testing performed.[1]
		Inspected the compliance tool and determined the Code of Conduct is communicated continuously to active employees and contractors through the compliance tool.	No exceptions noted.
CC1.5.3	The company's managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of active employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.
CC1.5.4	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	Inspected the company's Information Security Roles and Responsibilities Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned.	No exceptions noted.
CC1.5.5	The company requires new employees and contractors to complete security awareness training at the time of hire and active employees and contractors to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.5.5 (*cont.*)	The company requires new employees and contractors to complete security awareness training at the time of hire and active employees and contractors to complete security training at least annually.	Inspected the training records for a sample of contractors to determine that the company required contractors to complete security awareness training at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's personnel listing, there were no newly hired employees during the examination period; therefore, no testing was performed.	No testing performed.[1]
		Per inquiry with management and inspection of company's compliance tool, the annual security awareness training for active employees and contractors was completed in September 2024; therefore, no testing was performed.	No testing performed.[2]

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.1 – COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC2.1.2	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC2.1.3	The company utilizes a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	No exceptions noted.
CC2.2 – COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	Inspected the company's Information Security Roles and Responsibilities Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned.	No exceptions noted.
CC2.2.3	The company requires new employees and contractors to complete security awareness training at the time of hire and active employees and contractors to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Inspected the training records for a sample of contractors to determine that the company required contractors to complete security awareness training at the time of hire.	No exceptions noted.
		Per inquiry with management and inspection of the company's personnel listing, there were no newly hired employees during the examination period; therefore, no testing was performed.	No testing performed.[1]
		Per inquiry with management and inspection of company's compliance tool, the annual security awareness training for active employees and contractors was completed in September 2024; therefore, no testing was performed.	No testing performed.[2]

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2.4	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC2.2.5	The company describes its products and services to internal and external users.	Inspected the company's website to determine that the company provided a description of its products and services to internal and external users.	No exceptions noted.
CC2.2.6	The company communicates system changes to authorized internal users.	Inspected the internal communication channel to determine that the company communicated system changes to authorized internal users.	No exceptions noted.
CC2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The company's security commitments are communicated to customers in the Terms of Service (TOS) and Privacy Policy.	Inspected the Terms of Service (TOS) and Privacy Policy to determine that the company's security commitments were communicated to customers.	No exceptions noted.
CC2.3.2	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company's website to determine that the company provides guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
CC2.3.3	The company describes its products and services to internal and external users.	Inspected the company's website to determine that the company provided a description of its products and services to internal and external users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.3.4	The company has contact information on its website to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the company's website to determine that the company had contact information on their website to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
CC2.3.5	The company has written agreements in place with vendors and related third parties used for production. These agreements include security and confidentiality commitments applicable to that entity.	Inspected the Terms of Service for vendors to determine that security and confidentiality commitments were in place for vendors and related third parties used for production.	No exceptions noted.
CC2.3.6	The company notifies customers of critical system changes that may affect their processing.	Inspected the company's website to determine that the company notified customers of critical system changes that may affect their processing.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.1 – COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the annual security risk assessment and risk management policy to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC3.1.2	The company has a documented risk management policy 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 company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.1.3	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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.2 – COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	The company has a documented risk management policy 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 company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.2.2	The company has a third-party management policy in place. Components of this policy include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and subservice organizations.	Inspected the company's Third-Party Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.2.3	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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.2.4	The company has a documented business continuity/disaster recovery (BC/DR) Plan and tests it at least annually.	Inspected the company's BC/DR Plan to determine that the company has a documented BC/DR plan.	No exceptions noted.
		Per inquiry with management and inspection of the latest Tabletop Exercise Report, the annual BC/DR test was last performed in September 2024; therefore, no testing was performed.	No testing performed.[2]

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.3 – COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.3.2	The company has a documented risk management policy 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 company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.4 – COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.4.2	The company has a documented risk management policy 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 company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.1 – COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC4.1.2	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	**Exception noted.** A penetration test was not performed within the 12-month window in accordance with the Operations Security Policy.
CC4.1.3	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan report to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Inspected the completed vulnerability scan report to determine that the remediation plan was developed, and changes were implemented to remediate critical and high vulnerabilities in accordance with SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.1.4	The company has a third-party management policy in place. Components of this policy include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and subservice organizations.	Inspected the company's Third-Party Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	No exceptions noted.
CC4.2 – COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC4.2.2	The company has a third-party management policy in place. Components of this policy include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and subservice organizations.	Inspected the company's Third-Party Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.2.2 (*cont.*)	The company has a third-party management policy in place. Components of this policy include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and subservice organizations.	Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	No exceptions noted.
CC4.2.3	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	**Exception noted.** A penetration test was not performed within the 12-month window in accordance with the Operations Security Policy.
CC4.2.4	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	No exceptions noted.
		Inspected the remediation ticket/notes to determine that the remediation plan was developed, and changes were implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.1 – COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	The company has a documented risk management policy 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 company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.1.2	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC5.1.3	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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.1.4	Role-based access is configured within AWS and other supporting applications to enforce the segregation of duties and restrict access to confidential information.	Inspected the system configuration for AWS and other supporting applications to determine that role-based access was configured to enforce segregation of duties and restrict access to confidential information.	No exceptions noted.
CC5.2 – COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	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 company's Access Control Policy to determine that the Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC5.2.2	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 company's Operations Security and Secure Development policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC5.2.3	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.3 – COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC5.3.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Operations Security and Secure Development policies to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Per inquiry with management and inspection of compliance platform, there were no code, system, or infrastructure changes in the production environment during the examination period; therefore, no testing was performed.	No testing performed.[1]

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.3.3	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 company's Operations Security and Secure Development policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC5.3.4	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC5.3.5	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the annual security risk assessment to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC5.3.6	The company has a documented risk management policy 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 company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.3.7	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	Inspected the company's Information Security Roles and Responsibilities Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned.	No exceptions noted.
CC5.3.8	The company has a third-party management policy in place. Components of this policy include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and subservice organizations.	Inspected the company's Third-Party Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	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 company's Access Control Policy to determine that the Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.1.2	The company has a Data Management Policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the company's Data Management Policy to determine that the company had a Data Management Policy in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
CC6.1.3	The company's databases housing sensitive customer data are encrypted at rest.	Inspected the encryption configurations to determine that the company databases housing sensitive customer data are encrypted at rest.	No exceptions noted.
CC6.1.4	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the company's Cryptography Policy to determine that the company restricted privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
		Inspected the list of users with privileged access to encryption keys to determine that the company restricted privileged access to authorized users with a business need.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.1.5	Role-based access is configured within AWS and other supporting applications to enforce the segregation of duties and restrict access to confidential information.	Inspected the system configuration for AWS and other supporting applications to determine that role-based access was configured to enforce segregation of duties and restrict access to confidential information.	No exceptions noted.
CC6.1.6	The company restricts privileged access to the network, application, databases, and supporting cloud infrastructure to authorized users with a business need.	Inspected the list of users with privileged access to the cloud infrastructure and application to determine that the company restricted privileged access to the network, application, databases, and supporting cloud infrastructure to authorized users with a business need.	No exceptions noted.
CC6.1.7	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the list of users with privileged access to the firewall to determine that the company restricted privileged access to the firewall to authorized users with a business need.	No exceptions noted.
CC6.1.8	The firewall is configured to prevent unauthorized access to the company's network.	Inspected the firewall rules to determine that the firewall was configured to prevent unauthorized access to the company's network.	No exceptions noted.
CC6.1.9	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the access of sample of active employees and contractors to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.1.10	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the password configurations and written password policy to determine that the company required passwords for in-scope system components to be configured according to the company's policy.	No exceptions noted.
CC6.1.11	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the MFA configurations to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method.	No exceptions noted.
CC6.1.12	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.1.13	The company maintains a formal inventory of production system assets.	Inspected an inventory listing of information assets to determine that the company maintained a formal inventory of production system assets.	No exceptions noted.
CC6.1.14	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the network logs to determine that the company's network was segmented to prevent unauthorized access to customer data.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
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.			
CC6.2.1	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 company's Access Control Policy to determine that the Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.2.2	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the user access review documentation to determine that the company conducted quarterly access reviews for the in-scope system components to help ensure that access was restricted appropriately. Required changes are tracked to completion.	No exceptions noted.
CC6.2.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.	Inspected the user access and offboarding checklist and in-scope user listings for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process within the company's SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.2.4	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the access of sample of active employees and contractors to determine that the company ensured that user access to in-scope system components was based on job role and function.	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.			
CC6.3.1	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 company's Access Control Policy to determine that the Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.3.2	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the user access review documentation to determine that the company conducted quarterly access reviews for the in-scope system components to help ensure that access was restricted appropriately. Required changes are tracked to completion.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.3.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.	Inspected the user access and offboarding checklist and in-scope user listings for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process within the company's SLAs.	No exceptions noted.
CC6.3.4	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the access of sample of active employees and contractors to determine that the company ensured that user access to in-scope system components was based on job role and function.	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.			
CC6.4.1	Management contracts with Amazon Web Services (AWS) to provide physical access security of its production systems; therefore, this criterion is the responsibility of subservice organization.	This control activity is the responsibility of the subservice organization. Refer to the Subservice Organization section above for controls managed by the subservice organization.	
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.			
CC6.5.1	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 retention and disposal procedures to determine that the company had formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.5.2	The company has electronic media containing confidential information purged or destroyed in accordance with best practices.	Per inquiry with management and inspection of data disposal tracker, there were no disposals during the examination period; therefore, no testing was performed	No testing performed.[1]
CC6.5.3	The destruction of physical assets hosting the production environment is the responsibility of Amazon Web Services (AWS); therefore, part of this criterion is the responsibility of subservice organization.	This control activity is the responsibility of the subservice organization. Refer to the Subservice Organization section above for controls managed by the subservice organization.	
CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.6.2	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the MFA configurations to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method.	No exceptions noted.
CC6.6.3	The firewall is configured to prevent unauthorized access to the company's network.	Inspected the firewall rules to determine that the firewall was configured to prevent unauthorized access to the company's network.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.6.4	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificate to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.6.5	The company uses an Intrusion Detection System (IDS) to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations to determine that the company used an IDS to provide continuous monitoring of the company's network and early detection of potential security breaches.	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.			
CC6.7.1	The company encrypts portable media devices when used.	Inspected the company's Data Management Policy and Cryptography Policy to determine that the company encrypted portable media devices when used.	No exceptions noted.
		Inspected the encryption configurations for a representative sample of devices to determine that the company encrypted portable media devices when used.	No exceptions noted.
CC6.7.2	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificate to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.7.3	The company has a mobile device monitoring system in place to centrally monitor mobile devices supporting the service.	Inspected the company's mobile device monitoring system to determine that the company had a mobile device monitoring system in place to centrally monitor mobile devices supporting the service.	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.			
CC6.8.1	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks. The anti-malware software is configured to scan workstations daily and install updates as new updates/signatures are available.	Inspected the anti-malware configurations for a sample of workstations to determine that the company deployed anti-malware technology to environments commonly susceptible to malicious attacks.	No exceptions noted.
		Inspected the anti-malware configurations for a sample of workstations to determine that the anti-malware software was configured to scan workstations daily and install updates as new updates/signatures were available.	No exceptions noted.
CC6.8.2	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 company's Operations Security and Secure Development policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Operations Security and Secure Development policies to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Per inquiry with management and inspection of compliance platform, there were no code, system, or infrastructure changes in the production environment during the examination period; therefore, no testing was performed.	No testing performed.[1]
CC7.1.2	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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.1.3	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan report to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Inspected the completed vulnerability scan report to determine that the remediation plan was developed, and changes were implemented to remediate Critical and high vulnerabilities in accordance with SLAs.	No exceptions noted.
CC7.1.4	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	**Exception noted.** A penetration test was not performed within the 12-month window in accordance with the Operations Security Policy.
CC7.1.5	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's Operations Security Policy to determine that the company had a configuration management procedure in place to ensure that system configurations were deployed consistently throughout the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.1.6	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's Operations Security Policy to determine that the company's formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	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.			
CC7.2.1	The company uses an Intrusion Detection System (IDS) to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations to determine that the company used an IDS to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC7.2.2	The company utilizes a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	No exceptions noted.
CC7.2.3	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's Operations Security Policy to determine that the company's formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.2.4	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the monitoring tool configurations to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met.	No exceptions noted.
CC7.2.5	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan report to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Inspected the completed vulnerability scan report to determine that the remediation plan was developed, and changes were implemented to remediate Critical and high vulnerabilities in accordance with SLAs.	No exceptions noted.
CC7.2.6	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	**Exception noted.** A penetration test was not performed within the 12-month window in accordance with the Operations Security Policy.
CC7.2.7	Security incidents are reported to the IT personnel and tracked through to resolution in a ticketing system.	Per inquiry with management and inspection of incident response program, there were no incidents that occurred during the examination period; therefore, no testing was performed.	No testing performed.[1]

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC7.3.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Incident Response Plan to determine that the company's security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Per inquiry with management and inspection of incident response program, there were no incidents that occurred during the examination period; therefore, no testing was performed.	No testing performed.[1]
CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.4.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Incident Response Plan to determine that the company's security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Per inquiry with management and inspection of incident response program, there were no incidents that occurred during the examination period; therefore, no testing was performed.	No testing performed.[1]
CC7.4.3	The company has an approved Incident Response Plan and tests its incident response plan at least annually.	Inspected the company's Incident Response Plan to determine that the incident response plan was in place and approved by management.	No exceptions noted.
		Per inquiry with management and inspection of Tabletop Exercise Report, the annual Incident Response Plan test was last performed in September 2024; therefore, no testing was performed.	No testing performed.[2]
CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.5.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Incident Response Plan to determine that the company's security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Per inquiry with management and inspection of incident response program, there were no incidents that occurred during the examination period; therefore, no testing was performed.	No testing performed.[1]
CC7.5.3	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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC7.5.4	The company has a documented business continuity/disaster recovery (BC/DR) Plan and tests it at least annually.	Inspected the company's BC/DR Plan to determine that the company has a documented BC/DR plan.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.5.4 (*cont.*)	The company has a documented business continuity/disaster recovery (BC/DR) Plan and tests it at least annually.	Per inquiry with management and inspection of the latest Tabletop Exercise Report, the annual BC/DR test was last performed in September 2024; therefore, no testing was performed.	No testing performed.[2]

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	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 company's Operations Security and Secure Development policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC8.1.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Operations Security and Secure Development policies to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Per inquiry with management and inspection of compliance platform, there were no code, system, or infrastructure changes in the production environment during the examination period; therefore, no testing was performed.	No testing performed.[1]
CC8.1.3	Segregation of duties is in place to prevent developers from pushing changes to production.	Inspected the change management documentation for a software configuration ruleset to determine that segregation of duties was in place within the SDLC process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC8.1.4	The company restricts access to the production environment to authorized personnel.	Inspected the users with access to production to determine that the company restricts access to the production environment to authorized personnel.	No exceptions noted.
CC8.1.5	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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC8.1.6	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	**Exception noted.** A penetration test was not performed within the 12-month window in accordance with the Operations Security Policy.
CC8.1.7	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan report to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC8.1.7 (*cont.*)	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan report to determine that the remediation plan was developed, and changes were implemented to remediate Critical and high vulnerabilities in accordance with SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC9.1.2	The company has a documented risk management policy 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 company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC9.2: The entity assesses and manages risks associated with vendors and business partners			
CC9.2.1	The company has written agreements in place with vendors and related third parties used for production. These agreements include security and confidentiality commitments applicable to that entity.	Inspected the Terms of Service for vendors to determine that security and confidentiality commitments were in place for vendors and related third parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC9.2.2	The company has a third-party management policy in place. Components of this policy include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and subservice organizations.	Inspected the company's Third-Party Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and the subservice organization was performed annually.	No exceptions noted.

SECTION 5: OTHER INFORMATION PROVIDED BY RUBYWELL, INC.

OTHER INFORMATION PROVIDED BY RUBYWELL, INC.

Management Response to exception at CC4.1.2, CC4.2.3, CC7.1.4, CC7.2.6, and CC8.1.6.

Exception noted: A penetration test was not performed within the 12-month window in accordance with the Operations Security Policy.

Management's Response: Management acknowledges that the penetration test could have been performed during the audit period, as the development of new features did not introduce additional network exposure. The absence of a penetration test was a planned decision, not an oversight, as all software components were built within the past year. Our company strategically scheduled the penetration testing to coincide with system maturity. Until the penetration test is conducted, management maintained continuous threat detection and monitoring through AWS GuardDuty throughout the audit period.

For Commitment to Compliance and Improvement: Risk exposure was minimal as the system had no production users during this period and maintained standard security controls and continuous threat monitoring. A comprehensive penetration test will be conducted by Synack in March 2025 to address this exception.

For Process Enhancements Moving Forward: Management will prevent exception recurrence by establishing and adhering to an annual penetration testing schedule, with the next test scheduled for March 2026.