Insight Assurance

SOC 2 | ISO 27001 | PCI | HIPAA

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

Report on Coalesce Automation, Inc.'s Description of Its Management and Automation Service and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Throughout the Period May 1, 2024, to July 31, 2024

coalesce®

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT 1

INDEPENDENT SERVICE AUDITOR'S REPORT 2

SECTION 2: COALESCE AUTOMATION, INC.'S MANAGEMENT ASSERTION 6

COALESCE AUTOMATION, INC.'S MANAGEMENT ASSERTION 7

SECTION 3: COALESCE AUTOMATION, INC.'S DESCRIPTION OF ITS MANAGEMENT AND AUTOMATION SERVICE 9

COALESCE AUTOMATION, INC.'S DESCRIPTION OF ITS MANAGEMENT AND AUTOMATION SERVICE 10

SECTION 4: TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS 26

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY 28

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT

Insight Assurance
SOC 2 | ISO 27001 | PCI | HIPAA

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Coalesce Automation, Inc.

Scope

We have examined Coalesce Automation, Inc.'s ("Coalesce" or "the Service Organization") description of its Management and Automation Service found in Section 3 titled "Coalesce Automation, Inc.'s description of its Management and Automation Service" throughout the period May 1, 2024, to July 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 May 1, 2024, to July 31, 2024, to provide reasonable assurance that Coalesce'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.*

Coalesce uses Google Cloud Platform (GCP), Amazon Web Service (AWS) and Microsoft Azure 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 Coalesce, to achieve Coalesce's service commitments and system requirements based on the applicable trust services criteria. The description presents Coalesce's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Coalesce'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 Coalesce, to achieve Coalesce's service commitments and system requirements based on the applicable trust services criteria. The description presents Coalesce's controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of Coalesce'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.

Service Organization's Responsibilities

Coalesce is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that Coalesce's service commitments and system requirements were achieved. In Section 2, Coalesce has provided the accompanying assertion titled "Coalesce Automation, Inc.'s

Management Assertion" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Coalesce 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 system discusses its security incident response and recovery plan, which includes the controls implemented and operated to respond to and recover from security incidents. The Service Organization's security incident response plan includes procedures to help understand, contain, monitor, or eradicate a security incident, restore normal business operations in a timely manner with minimal, or no, business interruption or loss of data; and communicate with affected parties. However, during the period May 1, 2024, to July 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 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*, and CC7.5, *The entity identifies, develops, and implements activities to recover from identified security incidents.*

Our opinion is not modified with respect to the matter 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 Coalesce's Management and Automation Service that was designed and implemented throughout the period May 1, 2024, to July 31, 2024, in accordance with the description criteria.

- the controls stated in the description were suitably designed throughout the period May 1, 2024, to July 31, 2024, to provide reasonable assurance that Coalesce'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 Coalesce's controls throughout that period.
- the controls stated in the description operated effectively throughout the period May 1, 2024, to July 31, 2024, to provide reasonable assurance that Coalesce'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 Coalesce's controls operated effectively throughout that period.

Restricted Use

This report is intended solely for the information and use of Coalesce, user entities of Coalesce's Management and Automation Service throughout the period May 1, 2024, to July 31, 2024, and business partners of Coalesce subject to risks arising from interactions with the Management and Automation Service, 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
September 26, 2024

SECTION 2: COALESCE AUTOMATION, INC.'S MANAGEMENT ASSERTION



COALESCE AUTOMATION, INC.'S MANAGEMENT ASSERTION

We have prepared the description of Coalesce Automation, Inc.'s ("Coalesce" or "the Service Organization") Management and Automation Service entitled "Coalesce Automation, Inc.'s description of its Management and Automation Service" throughout the period May 1, 2024, to July 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 Management and Automation Service that may be useful when assessing the risks arising from interactions with Coalesce's system, particularly information about system controls that Coalesce 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.*

Coalesce uses Google Cloud Platform (GCP), Amazon Web Service (AWS) and Microsoft Azure 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 Coalesce, to achieve Coalesce's service commitments and system requirements based on the applicable trust services criteria. The description presents Coalesce's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Coalesce's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Coalesce, to achieve Coalesce'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 Coalesce's controls.

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

- the description presents Coalesce's Management and Automation Service that was designed and implemented throughout the period May 1, 2024, to July 31, 2024, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period May 1, 2024, to July 31, 2024, to provide reasonable assurance that Coalesce'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 Coalesce's controls

- the controls stated in the description operated effectively throughout the period May 1, 2024, to July 31, 2024, to provide reasonable assurance that Coalesce'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 Coalesce's controls operated effectively throughout that period.

Coalesce Automation, Inc.
September 26, 2024

SECTION 3: COALESCE AUTOMATION, INC.'S DESCRIPTION OF ITS MANAGEMENT AND AUTOMATION SERVICE

COALESCE AUTOMATION, INC.'S DESCRIPTION OF ITS MANAGEMENT AND AUTOMATION SERVICE

COMPANY BACKGROUND

DESCRIPTION OF SERVICES PROVIDED

Coalesce Automation, Inc. (the "company") provides management and automation services for Snowflake data warehouses. The company was founded in 2021 and provides the toolset to produce clean, up-to-date single source of truth datasets that can then be consumed by the rest of your business.

Coalesce's core product, Management and Automation Service (the "system") is a Software as a Service (SaaS) solution that includes the following components:

- Metadata Repository: Coalesce stores the metadata format for each of your data warehouse environments in a highly scalable NoSQL database. This metadata never stores Snowflake data or passwords, it is solely used for storing the metadata configuration of your data warehouse and storing deployment success and failure.
- Developer's GUI (Frontend): The Coalesce frontend communicates on behalf of users when they are logged in via app.coalescesoftware.io. It communicates to the metadata repository and submits commands to Snowflake on your behalf.
- CLI tool: For automation purposes, the CLI Tool is used for automating all transformations, enabling all data transformations to run on-premises.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

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

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

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

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system;
- Quarterly vulnerability scans over the system and network, and annual penetration tests over the production environment; and,
- 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.

Such requirements are communicated in Coalesce's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

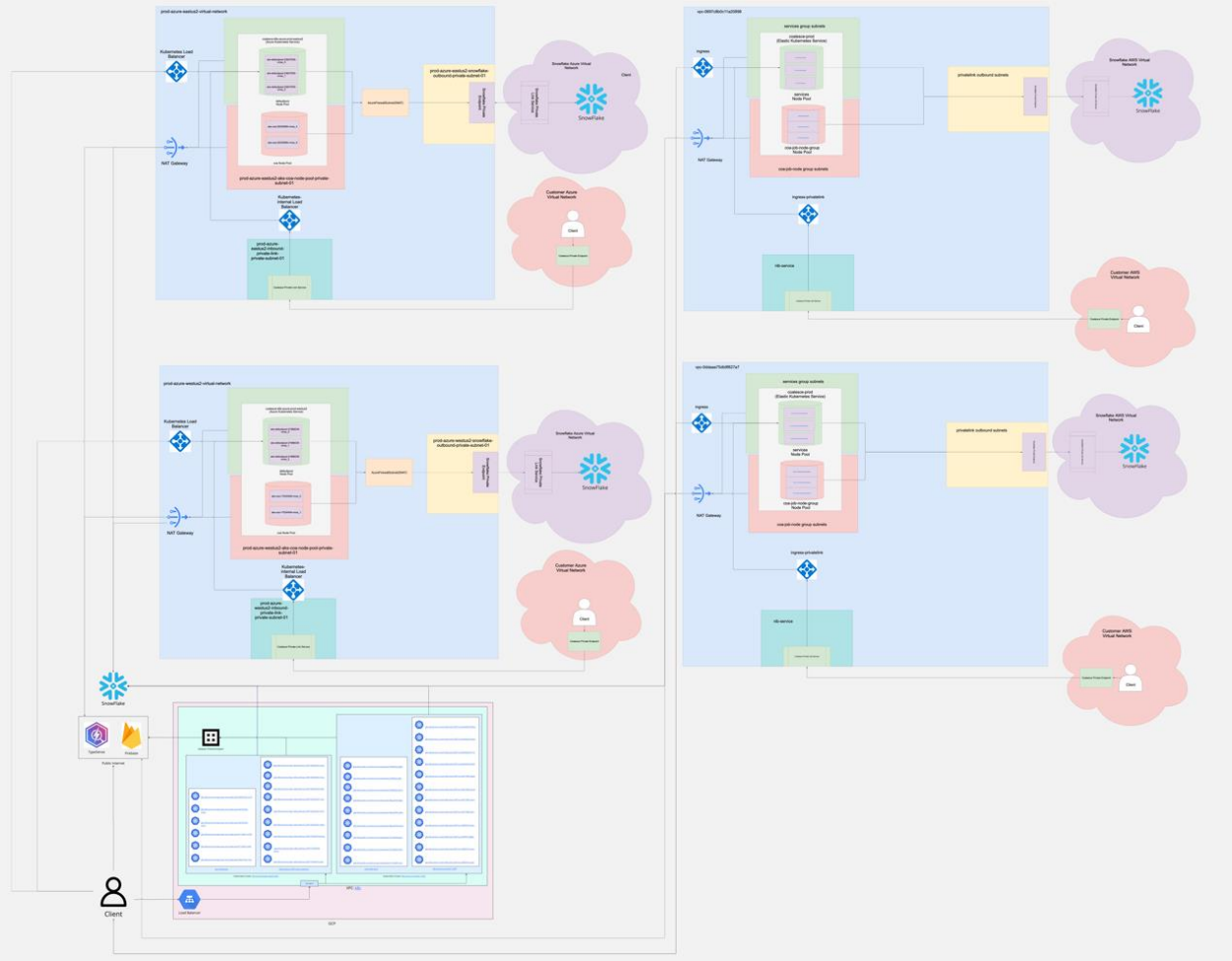
The purpose of the system description is to delineate the boundaries of the system, which includes the services and commitments outlined above and the five components described below: infrastructure, software, people, data, and processes and procedures.

INFRASTRUCTURE

The system is hosted in Google Cloud Platform (GCP) in a virtual private cloud (VPC) environment which protects the network from unauthorized external access. The network topology includes segmented VPCs and access control lists (ACLs). User requests to Coalesce's web-based systems are encrypted using Transport Layer Security (TLS) using certificates from an established third-party certificate authority. Remote system administration access to Coalesce production systems (including production Kubernetes clusters) is available through a virtual private network (VPN) connection. The hardware components that make up the aforementioned system include servers hosted, managed, and protected by GCP. GCP maintains failover capabilities in the event of physical hardware or logical software failures. This infrastructure is hosted in high availability data centers with multiple availability zones. Furthermore, the primary infrastructure encompasses other subservice organizations, including Amazon Web Services (AWS) and Microsoft Azure.

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Google Cloud Platform	Primary Cloud Infrastructure	Cloud Infrastructure Provider for the Coalesce application
Amazon Web Services (AWS)	Cloud Infrastructure	Supports primary cloud infrastructure
Microsoft Azure	Cloud Infrastructure	Supports primary cloud infrastructure

To outline the topology of its network, the organization maintains the following network diagram:



SOFTWARE

Coalesce is responsible for managing the development and operation of Coalesce's Management and Automation Service including software components such as servers, databases, and storage systems.

The in-scope Coalesce software components are shown in the table below:

Software Infrastructure		
System / Application	**Operating System DB**	**Purpose**
Coalesce Metadata Repository	Google Firestore	Stores the metadata format for each client data warehouse environments in a highly scalable NoSQL database.
Coalesce Developer's GUI (Frontend)	Linux / Kubernetes/ Google Firestore	The Coalesce frontend communicates on behalf of users when they are logged in via app.coalescesoftware.io. It communicates to the metadata repository and submits commands to Snowflake on the client's behalf.
Coalesce CLI Tool	Linux / Kubernetes/ Google Firestore	The Coalesce CLI Tool is used for automating all transformations, enabling data transformations to run on-premise.
GCP Firewalls	GCP Proprietary	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic.
Bitbucket	Bitbucket Proprietary	Source code repositories, version control systems, and build software.
Jenkins	Jenkins Proprietary	Source code repositories, version control systems, and build software.
Google Cloud DNS	GCP Proprietary	DNS service provided by GCP.
JIRA	Atlassian	A customizable tool for agile software development; logs and tracks progress for bugs, tasks, features, and projects.
Slack / G Suite	Salesforce / Google	Office communication services.
Datadog	Datadog Proprietary	Cloud monitoring, log aggregation, and alert generation service.
PagerDuty	PagerDuty Proprietary	Real time alerting service for on-call personnel.
Vanta	Vanta Proprietary	Security monitoring and compliance automation solution.
Snowflake	Snowflake Proprietary	Integrated application and data transformation.

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 in their specific tasks and on the ways to keep the company and its data secure.

Coalesce staff maintains the following functional areas:

- **Management –** Responsible for overseeing companywide activities, establishing, and accomplishing goals, and overseeing objectives.
- **Engineering –** Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.
- **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.
- **Security –** Responsible for access controls and security of the production environment.
- **People –** Responsible for recruiting and onboarding new personnel, defining roles and positions for new hires, performing background checks, and facilitating the employee termination process.
- **IT –** Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.
- **Customer Success –** Responsible for sales, account management, customer success, and customer support activities.

DATA

Data, as defined by Coalesce, constitutes the following:

1. App Data:
    - SQL transformation code
    - Database object schema structures
    - Error exception handling data
    - OAuth connection tokens
2. App Usage data

- Customer name
- Email
- IP address
- App feature usage

Information assets are assigned a sensitivity level based on the audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data is to be assigned one of the following categories:

Data Categorization		
Category	**Description**	**Examples**
Confidential	Highly sensitive data requiring the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner, or a company executive.	• Customer Data • Personally identifiable information (PII) • Company financial and banking data • Salary, compensation, and payroll information • Strategic plans • Incident reports • Risk assessment reports • Technical vulnerability reports • Authentication credentials • Secrets and private keys • Source code • Litigation data
Restricted	Coalesce Software proprietary information requiring thorough protection; access is restricted to employees with a “need-to-know” based on business requirements. This data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise.	• Internal policies • Legal documents • Meeting minutes and internal presentations • Contracts • Internal reports • Slack messages • Email
Public	Documents intended for public consumption which can be freely distributed outside Coalesce Software.	• Marketing materials • Product descriptions • Release notes • External facing policies

PROCESSES AND PROCEDURES

Management has developed and communicated policies and procedures to manage the information security of the system through best practice processes. Changes to these processes are performed annually and authorized by senior management. These processes cover the following key security life cycle areas:

- Access Control
- Asset Management
- Business Continuity and Disaster Recovery
- Code of Conduct
- Cryptography
- Data Management
- Human Resource Security
- Incident Response Plan
- Information Security
- Information Security Roles and Responsibilities
- Operations Security
- Physical Security
- Risk Management
- Secure Development
- Third-Party Management

Physical Security

Coalesce's production servers are maintained by AWS, Microsoft Azure and GCP. The physical and environmental security protections are the responsibility of AWS, Microsoft Azure and GCP. Coalesce reviews the attestation reports and performs a risk analysis of AWS, Microsoft Azure and GCP on at least an annual basis. Coalesce Office is protected with an access badge/access control.

System Monitoring

The Operations Security Policy and Secure Development Policy describe the organization's policies and procedures related to network logging and monitoring as well as vulnerability identification and remediation. The organization uses Microsoft Azure, GCP and CloudTrail for system logging within the Google environment, and the organization collects logs from the Redwood City office router and firewall. CloudWatch logs and the Redwood City office router and firewall logs document source IP, destination IP, destination port, protocol type, and timestamp. The organization monitors system capacity using an internal application monitoring platform.

CrowdStrike, AWS and GCP are 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 Penetration Testing, CIS testing, implementation of antivirus software, and system patching. The organization uses anti-virus software 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. GCP Security Command Center and GitHub Vulnerability Scanners are used to identify

newly emerging vulnerabilities, and the organization monitors vendors for patch updates to correct vulnerabilities.

Logical Access

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

Access to these systems is split into three levels: Administrator, User, and No Access. 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 Coalesce's policies and completing the security training.

When an employee is terminated, the offboarding Team is responsible for deprovisioning access to all in-scope systems on the same day of the employee's termination.

Change Management

Coalesce maintains documented 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. Testing is performed in an environment that is logically separated from the production environment. The Change Control Board approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Computer Operations

Customer data is backed up and monitored by the Engineering for completion and exceptions. If there is an exception, Engineering 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, GCP, and Microsoft Azure with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Coalesce 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.

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

Coalesce 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.

Data Communications

Coalesce performs quarterly vulnerability scans and annual penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the standard incident response and change management process.

Patch Management

Coalesce takes a proactive approach to patch management. The IT/Security Team and Engineering leadership team continuously monitor various websites, message boards, and mailing lists where advanced notifications of bug-related patches are often disclosed prior to a public announcement by the vendor. In addition, patches are tested for stability prior to production deployment. This allows the company to plan for rollouts of planned patches.

Backup And Recovery

Customer data is backed up and monitored by the operations for completion and exceptions. If there is an exception, operations 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, GCP, and Microsoft Azure with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Problem Management

Coalesce 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. 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 incident response training.

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 Coalesce's Management and Automation Service 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 Coalesce's Management and Automation Service.

This report does not include the Cloud Hosting Services provided by Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure at multiple facilities.

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

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section 4, they are an integral part of Coalesce's description of the system. This section provides information about the five interrelated components of internal control at Coalesce, including:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring controls

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 assure 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

Coalesce has developed a Code of Conduct that addresses expected standards of ethical and moral behavior. The company has also developed employee confidentiality agreements that prohibit inappropriate use and disclosure of customer or company information. These documents are provided to all new employees and other personnel as needed. All employees are required to

sign an acknowledgement form that they received and agree to follow the Code of Conduct and confidentiality agreement within 30 days of hire and annually thereafter.

Executive Management Oversight

Coalesce's control awareness is significantly influenced by its executive management. Attributes that define "tone at the top" include executive management's experience of its members, their involvement and scrutiny of operational activities, and their interaction with independent assessments of the company's operations and information security posture.

Management's Philosophy and Operating Style

Coalesce's control environment reflects the philosophy of management. Coalesce's security function meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of executive management, oversees the security activities and communication of its policies and procedures.

Commitment to Competence

Coalesce'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

Management and employees are assigned levels of authority and responsibility to facilitate internal control. Each policy has an individual owner with accountability and authority over policy enforcement, supported by management. Organizational charts are in place to communicate key areas of authority, responsibility, and lines of reporting to personnel that support the design, development, implementation, operation, maintenance, and monitoring of the system. These charts are communicated to employees and updated automatically via an integration with Coalesce's Google Workspace.

Human Resource Policies and Practices

The company maintains formal hiring and termination policies and procedures. Candidates are evaluated through a formal interview process against the job position's job description. Background checks are performed on new hires prior to hire. New hires are required to

acknowledge their receipt of security policies, employee handbook, and confidentiality related agreements within 30 days of hire.

Within the first 30 days of hire and annually thereafter, all employees must complete training courses covering basic information security practices. The training courses are designed to assist employees in identifying and responding to social engineering attacks and in avoiding inappropriate security practices.

If an employee violates the Code of Conduct in the employee handbook or the company's policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.

Management evaluates employee performance on an annual basis against their job performance, job function, and company objectives.

RISK ASSESSMENT PROCESS

Coalesce annually reviews the risks that may threaten the achievement of its service commitments and system requirements.

The security function assesses security risks on an ongoing basis. This is done through management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting continuous risk assessment using tool assisted analysis.

The annual risk assessment is communicated by the security function and approved by senior management. As part of the assessment, risks affecting the organization and recommended courses of action are identified and discussed. Where applicable, mitigating controls are recommended and implemented to address the risks.

Management considers the potential for fraud when assessing the risks to the company's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts such as violations of governmental laws.

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, management considers fraud factors in each risk evaluated during the risk assessment process.

Senior management, as part of its annual Information Security Policy review, considers developments in technology and the impact of applicable laws and regulations on Coalesce's security policies. Security risks related to external parties (such as contractors and vendors) are identified and addressed based on its procurement and third-party risk management program. Designated responsibilities are defined in reviewing risks associated with external parties and establishing relevant agreements.

Coalesce has a process in place for evaluating vendor performance and compliance with contractual obligations. Related party and vendor systems are subject to review annually as part of the vendor risk management process. Attestation reports (SOC 2 reports) are evaluated when available.

Changes in security threats and risks are reviewed by Coalesce, and updates to existing control activities and information security policies are performed, as necessary.

Integration with Risk Assessment

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

INFORMATION AND COMMUNICATION

Coalesce has an Information Security Policy to help ensure employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

MONITORING CONTROLS

In addition to the daily oversight, information security key performance indicators are defined and continuously monitored using compliance automation software. Monitoring results are reviewed for compliance status (i.e., SLAs, patch levels, security awareness compliance, high risk vulnerabilities, etc.).

On-going Monitoring

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

Monitoring of the Subservice Organization

Coalesce uses a subservice organization to provide hosting services.

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

Reporting Deficiencies

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

Annual risk meetings are held for management to review reported deficiencies and corrective actions.

TRUST SERVICES CATEGORY

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 Security criteria are included in Section 4 of this report and are an integral part of the description of the system.

CONTROL ACTIVITIES AND CRITERIA

The Company's trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancies that would result from listing them here in Section 3 and repeating them in Section 4. Although the trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Coalesce's description of controls.

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

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)

Coalesce uses subservice organizations in support of its system. Coalesce's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the Coalesce system to be achieved solely by Coalesce. Therefore, user entity controls must be evaluated in conjunction with Coalesce's controls 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, GCP and Azure are responsible for maintaining physical security and environmental protection controls over the data centers hosting the Coalesce's infrastructure.	CC6.4
2.	AWS, GCP and Azure are responsible for the destruction of physical assets hosting the production environment.	CC6.5

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Coalesce controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain trust services criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for the processing of transactions for Coalesce customers.

For customers to rely on the information processed through the Coalesce system, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures and controls should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

1. User entity is responsible for protecting established user credentials within their organizations.
2. User entity is responsible for reviewing customer access to the Coalesce system periodically to validate appropriateness of access levels.
3. User entity is responsible for approving and creating new user access to the Coalesce system.
4. User entity is responsible for removing terminated employee access to the Coalesce system.
5. User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into the Coalesce system.
6. User entity is responsible for sending data to Coalesce via a secure connection and/or the data should be encrypted.

7. User entity is responsible for notifying Coalesce if they detect or suspect a security incident related to the Coalesce system.
8. User entity is responsible for reviewing email and other forms of communications from Coalesce, related to changes that may affect Coalesce customers and users, and their security or availability obligations.
9. User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the system.
10. User entity is responsible for endpoint protection of workstations used to access the system.
11. User entity is responsible for developing their own business continuity and disaster recovery plan.

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 May 1, 2024, to July 31, 2024.

The trust services criteria for the Security category and related controls specified by Coalesce 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 control was performed outside 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 Test 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 to determine that the company had an approved Code of Conduct that is reviewed annually and updated as needed.	No exceptions noted.
		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 employees and contractors to acknowledge the Code of Conduct at the time of hire.	Inspected the Code of Conduct acknowledgment for a sample of new employees to determine that the Code of Conduct was acknowledged at the time of hire.	No exceptions noted.
CC1.1.3	The company requires employees to review and acknowledge the information security policies at the time of hire.	Inspected the information security policies acknowledgment for a sample of new employees and contractors to determine that the information security policies were acknowledged at the time of hire.	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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC1.1.5	The company performs background checks on new employees.	Inspected the completed background check for a sample of new employees to determine whether the company performed background checks on new employees.	No exceptions noted.
CC1.1.6	Employees are required to review and acknowledge the confidentiality agreement at the time of hire.	Inspected the confidentiality agreement for a sample of new employees to determine that employees were required to review and acknowledge the confidentiality agreement at the time of hire.	No exceptions noted.
CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls.	Inspected the board members' profiles to determine that the company's board members had sufficient expertise to oversee management's ability to design, implement and operate information security controls.	No exceptions noted.
CC1.2.2	The company's board of directors meets annually and maintains formal meeting minutes.	Per inquiry with management and inspection of the latest Board of Director meeting minutes, the Board of Director formal meeting was performed on November 13, 2023. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
CC1.2.3	The company's board of directors has a documented Information Security Roles and Responsibilities Policy that outlines its	Inspected the company's Information Security Roles and Responsibilities Policy to determine that the company's board of directors had a	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
	oversight responsibilities for internal control.	documented Information Security Roles and Responsibilities Policy that outlined its oversight responsibilities for internal control.	
CC1.2.4	The company's board of directors consists of members that are independent of the company.	Inspected the board of directors listing to determine that the company's board of directors consisted of members that were independent of the company.	No exceptions noted.
CC1.3 –COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
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 job descriptions within the Information Security Roles and Responsibilities Policy.	Inspected the company's sample job description within the 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 in the job descriptions within the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC1.3.3	The company requires employees and contractors to review and acknowledge the	Inspected the information security policies acknowledgment for a sample of new employees and contractors to determine that the information	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
	information security policies at the time of hire.	security policies were acknowledged at the time of hire.	
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.	Inspected the completed background check for a sample of new employees to determine whether the company performed background checks on new employees.	No exceptions noted.
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 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 job descriptions within the Information Security Roles and Responsibilities Policy.	Inspected the company's sample job description within the 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 in the job descriptions within the Information Security Roles and Responsibilities Policy.	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	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
	employees to complete security training at least annually.	information security topics and the latest trends to protect sensitive data.	
		Inspected the training records for a sample of new employees and contractors to determine that the company required employees and contractors to complete security awareness training at the time of hire.	No exceptions noted.
		Inspected the training records for a sample of active employees to determine that the company required employees to complete security awareness training annually.	No exceptions noted.
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 to determine that the company had an approved Code of Conduct that is reviewed annually and updated as needed.	No exceptions noted.
		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 employees and contractors to acknowledge the Code of Conduct at the time of hire.	Inspected the Code of Conduct acknowledgment for a sample of new employees and 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 Test of Controls**	**Test Results**
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 job descriptions within the Information Security Roles and Responsibilities Policy.	Inspected the company's sample job description within the 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 in job descriptions within the Information Security Roles and Responsibilities Policy.	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 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 new employees and contractors to determine that the company required employees and contractors to complete security awareness training at the time of hire.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test 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 to complete security training at least annually.	Inspected the training records for a sample of active employees to determine that the company required active employees to complete security awareness training annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Test 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.	Per inquiry with management and inspection of information security policies and procedures tracked within Vanta, review was performed on March 25, 2024. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
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	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
		and procedures that were documented and communicated to authorized users.	
CC2.2.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions within the Information Security Roles and Responsibilities Policy.	Inspected the company's sample job description within the 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 in the job descriptions within the Information Security Roles and Responsibilities Policy.	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 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 new employees and contractors to determine that the company required employees and contractors to complete security awareness training at the time of hire.	No exceptions noted.
		Inspected the training records for a sample of active employees to determine that the company required active employees to complete security awareness training annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC2.2.4	The company's information security policies and procedures are documented and reviewed at least annually.	Per inquiry with management and inspection of information security policies and procedures tracked within Vanta, review was performed on March 25, 2024. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
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/example communication 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 Security Information Page and Terms of Service (TOS).	Inspected the Security Information Page and TOS to determine that the company's security commitments were communicated to customers in the Security Information Page and TOS.	No exceptions noted.
CC2.3.2	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company's support page/knowledge base to determine that the company provides guidelines and technical	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
		support resources relating to system operations to customers.	
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 described its products and services to internal and external users.	No exceptions noted.
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 the 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. These agreements include security and confidentiality commitments applicable to that entity.	Inspected the Terms of Service and Privacy Policy for vendors to determine that security and confidentiality commitments were in place for vendors and related third parties.	No exceptions noted.
CC2.3.6	The company notifies customers of critical system changes that may affect their processing.	Inspected 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 Test 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 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 program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the 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.	Per inquiry with management and inspection of the Risk Report in Vanta, the most recent risk assessment was performed on March 13, 2024. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Test 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 program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the 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 program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors	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 was performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Test 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.	Per inquiry with management and inspection of the Risk Report in Vanta, the most recent risk assessment was performed on March 13, 2024. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
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 BC/DR Plan tabletop exercise meeting minutes, the company tested the BC/DR Plan on December 4, 2023. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
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	Per inquiry with management and inspection of the Risk Report in Vanta, the most recent risk assessment was performed on March 13, 2024.	No testing performed[2].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
	(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.	As a result, the control did not operate during the examination period. Therefore, no testing was performed.	
CC3.3.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the 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.
CC3.4 – 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	Per inquiry with management and inspection of the Risk Report in Vanta, the most recent risk assessment was performed on March 13, 2024. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
	how fraud may impact the achievement of objectives.		
CC3.4.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the 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 Test 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.	Per inquiry with management and inspection of the Summit Security Group penetration report, the latest penetration test was performed on November 3, 2023. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
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 remediation ticket/notes for a sample of vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.
CC4.1.4	The company has a third-party management program in place. Components of this program include: - critical vendor inventory.	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 Test of Controls**	**Test Results**
	- vendor's security requirements; and - annual review of critical vendors	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 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 program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors	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 was performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
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.	Per inquiry with management and inspection of the Summit Security Group penetration report, the latest penetration test was performed on November 3, 2023. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
CC4.2.4	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 remediation ticket/notes for a sample of vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test 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 program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the 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.	Per inquiry with management and inspection of information security policies and procedures tracked within Vanta, review was performed on March 25, 2024. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
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.	Per inquiry with management and inspection of the Risk Report in Vanta, the most recent risk assessment was performed on March 13, 2024. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC5.1.4	Role-based access is configured within Amazon Web Services (AWS), GCP, and Microsoft Azure and other supporting applications to enforce the segregation of duties and restrict access to confidential information.	Inspected the system configuration for Amazon Web Services (AWS), GCP, and Microsoft Azure, 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.	Per inquiry with management and inspection of information security policies and procedures tracked within Vanta, review was performed on	No testing performed[2].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
		March 25, 2024. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	
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.	Per inquiry with management and inspection of information security policies and procedures tracked within Vanta, review was performed on March 25, 2024. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
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.
		Inspected the change management documentation for a sample of changes 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC5.3.3	The company has a formal 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 program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the 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 Test 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 job descriptions within the Information Security Roles and Responsibilities Policy.	Inspected the company's sample job description within the 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 in the job descriptions within the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC5.3.8	The company has a third-party management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors	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 was performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test 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 Test of Controls**	**Test Results**
CC6.1.5	Role-based access is configured within Amazon Web Services (AWS), GCP, and Microsoft Azure and other supporting applications to enforce the segregation of duties and restrict access to confidential information.	Inspected the system configuration for Amazon Web Services (AWS), GCP, and Microsoft Azure 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 user access request and in-scope user listings for a sample of new 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 Test 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 VPC 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 Test 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 reviews for the in-scope system components to help ensure that access was restricted appropriately.	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.
CC6.2.4	The company ensures that user access to in-scope system components is based on job role and function.	Inspected the user access request and in-scope user listings for a sample of new 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 Test of Controls**	**Test Results**
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.	No exceptions noted.
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 user access request and in-scope user listings for a sample of new 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 Test of Controls**	**Test Results**
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), GCP, and Microsoft Azure to provide physical access security of its production systems.	This control is the responsibility of the Subservice Organizations. Refer to the Subservice Organization's section above for controls managed by the Subservice Organizations.	
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.
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 media disposal listing managed by the company, there were no disposals performed during the examination period. As a result, the control did not occur 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), GCP, and Microsoft Azure.	This control is the responsibility of the Subservice Organizations. Refer to the Subservice Organization's section above for controls managed by the Subservice Organizations.	

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
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 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.
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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
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 and removable media devices when used.	Inspected the company's Cryptography Policy to determine that the company encrypted portable and removable media devices when used.	No exceptions noted.
		Inspected the encryption configurations for a 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.
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-	Inspected the anti-malware configurations for a sample of workstations to determine that the company deployed anti-malware technology to	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
	malware software is configured to scan workstations daily and install updates as new updates/signatures are available.	environments commonly susceptible to malicious attacks.	
		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 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 Test 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.
		Inspected the change management documentation for a sample of changes 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.
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.	Per inquiry with management and inspection of the Risk Report in Vanta, the most recent risk assessment was performed on March 13, 2024. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test 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 remediation ticket/notes for a sample of vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	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.	Per inquiry with management and inspection of the Summit Security Group penetration report, the latest penetration test was performed on November 3, 2023. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
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.
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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	The company uses an 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.
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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
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 remediation ticket/notes for a sample of vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	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.	Per inquiry with management and inspection of the Summit Security Group penetration report, the latest penetration test was performed on November 3, 2023. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
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 listing managed by the company, there were no incidents reported during the examination period. As a result, the control did not occur during the examination period. Therefore, no testing was performed.	No testing performed[1].
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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
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 listing managed by the company, there were no incidents reported during the examination period. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing peformed[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.
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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
		Per inquiry with management and inspection of incident listing managed by the company, there were no incidents reported during the examination period. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing peformed[1].
CC7.4.3	The company has a documented Incident Response Plan and tests it 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 the meeting notes from the latest Incident Response Plan Test meeting, the last Incident Response Plan test was performed on December 4, 2023. As a result, the control did not operate during the examination period. 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.
CC7.5.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the	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	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
	company's security incident response policy and procedures.	management according to the company's security incident response policy and procedures.	
		Per inquiry with management and inspection of incident listing managed by the company, there were no incidents reported during the examination period. As a result, the control did not occur 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.	Per inquiry with management and inspection of the Risk Report in Vanta, the most recent risk assessment was performed on March 13, 2024. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
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.
		Per inquiry with management and inspection of the latest BC/DR Plan tabletop exercise meeting minutes, the company tested the BC/DR Plan on December 4, 2023. As a result, the control did	No testing performed[2].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
		not operate during the examination period. Therefore, no testing was performed.	

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Test 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 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.
		Inspected the change management documentation for a sample of changes 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.
CC8.1.3	Segregation of duties is in place to prevent developers from pushing changes to production.	Inspected the branch protection settings and change management documentation for a	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
		sample of changes to determine that segregation of duties was in place within the SDLC process.	
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.	Per inquiry with management and inspection of the Risk Report in Vanta, the most recent risk assessment was performed on March 13, 2024. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
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.	Per inquiry with management and inspection of the Summit Security Group penetration report, the latest penetration test was performed on November 3, 2023. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
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.
		Inspected the remediation ticket/notes for a sample of vulnerabilities to determine that critical	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
		and high vulnerabilities were tracked to remediation.	

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Test 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.	Per inquiry with management and inspection of the Risk Report in Vanta, the most recent risk assessment was performed on March 13, 2024. As a result, the control did not operate during the examination period. Therefore, no testing was performed.	No testing performed[2].
CC9.1.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the 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. These agreements include security and confidentiality commitments applicable to that entity.	Inspected the Terms of Service and Privacy Policy 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 Test of Controls**	**Test Results**
CC9.2.2	The company has a third-party management program in place. Components of this program include: - critical inventory. - vendor's security requirements; and - annual review of critical vendors	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 was performed annually.	No exceptions noted.