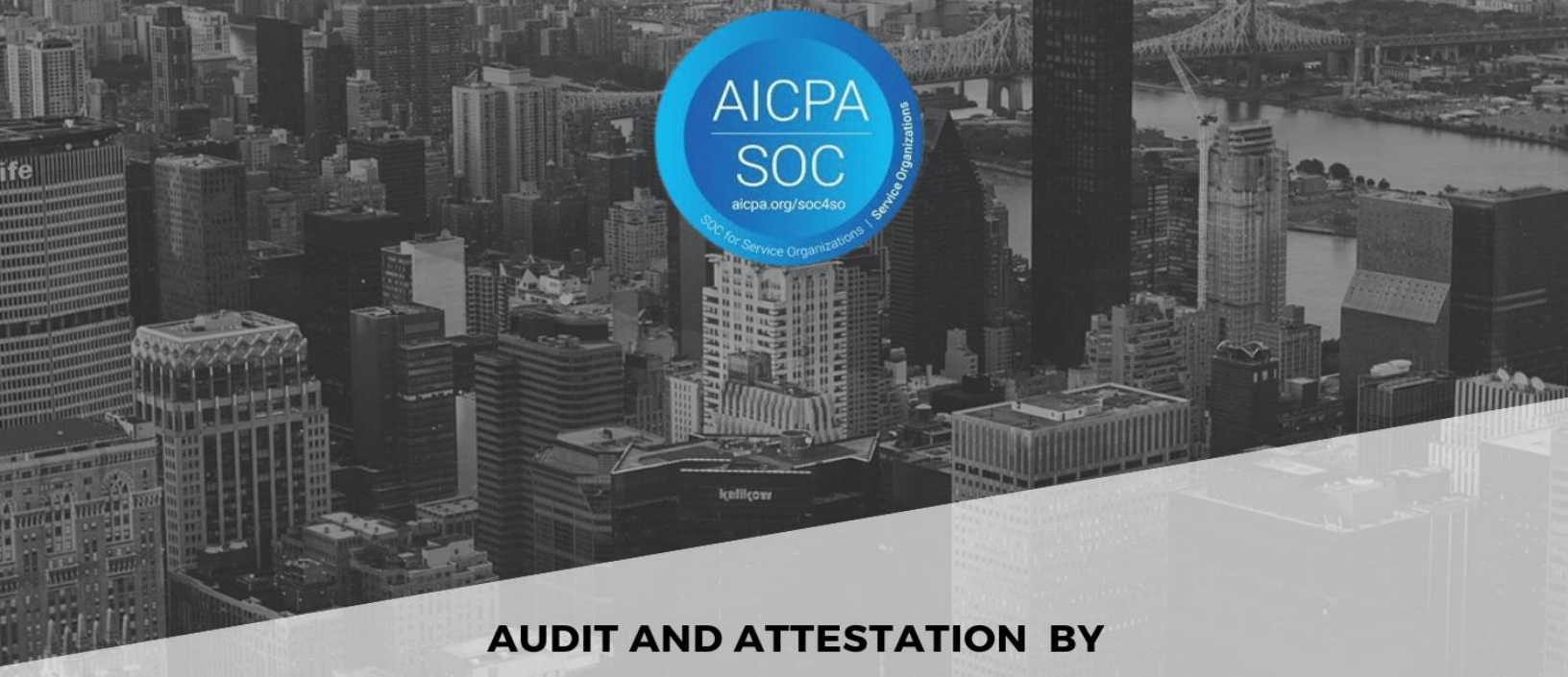
SOC 2 Type 2 Report

Kolide, Inc.

January 1, 2023 to June 30, 2023
Next Audit Observation End Date: June 30, 2024

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



AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA™

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

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

AICPA NOTICE:

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

The next report would be issued on September 29, 2024 subject to observation and examination by Prescient Assurance.

Table of Contents

SECTION 1

Management's Assertion

Management's Assertion

We have prepared the accompanying description of Kolide, Inc.'s system throughout the period January 1, 2023 to June 30, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. The description is intended to provide report users with information about Kolide, Inc.'s system that may be useful when assessing the risks arising from interactions with Kolide, Inc.'s system, particularly information about system controls that Kolide, Inc. has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

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

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

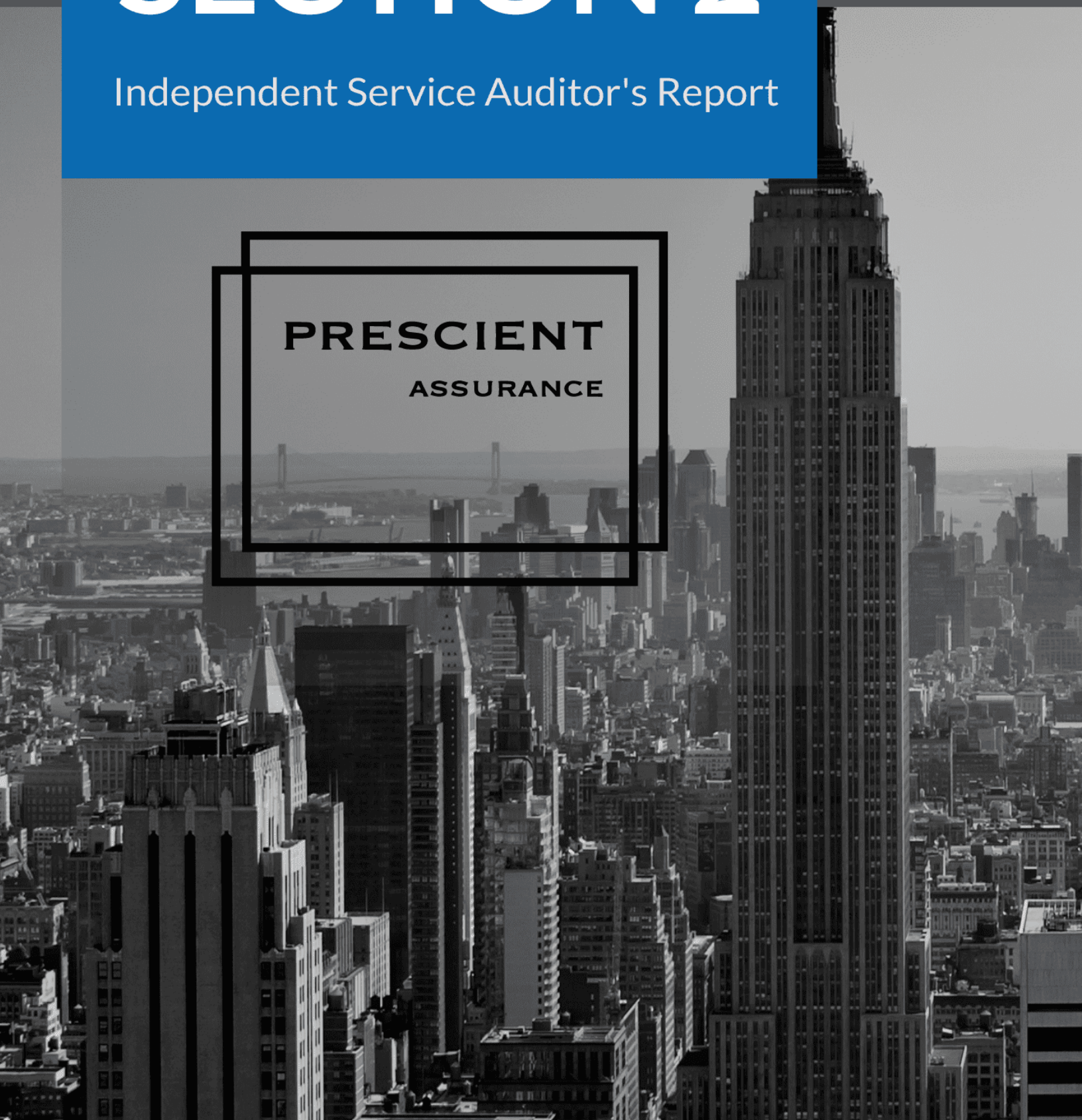
a. The description presents Kolide, Inc.'s system that was designed and implemented throughout the period January 1, 2023 to June 30, 2023 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period January 1, 2023 to June 30, 2023, to provide reasonable assurance that Kolide, Inc's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Kolide, Inc.'s controls during that period.
c. The controls stated in the description operated effectively throughout the period January 1, 2023, to June 30, 2023, to provide reasonable assurance that Kolide, Inc's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of Kolide, Inc.'s controls operated effectively throughout the period.

DocuSigned by:
Antigoni Sinanis
67AC8F90G314440...

Antigoni Sinanis
Director of Operations
Kolide, Inc.

SECTION 2

Independent Service Auditor's Report



Independent Service Auditor's Report

To: Kolide, Inc.

Scope

We have examined Kolide, Inc.'s ("Kolide, Inc.") accompanying description of its Kolide system found in Section 3, titled Kolide, Inc. System Description throughout the period January 1, 2023, to June 30, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2023, to June 30, 2023, to provide reasonable assurance that Kolide, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Confidentiality set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

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

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

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

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

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

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

Inherent Limitations

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

inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects:

a. The description presents Kolide, Inc.'s system that was designed and implemented throughout the period January 1, 2023, to June 30, 2023, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period January 1, 2023, to June 30, 2023, to provide reasonable assurance that Kolide, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of Kolide, Inc.'s controls throughout the period.
c. The controls stated in the description operated effectively throughout the period January 1, 2023, to June 30, 2023, to provide reasonable assurance that Kolide, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Kolide, Inc.'s controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of Kolide, Inc., user entities of Kolide, Inc.'s system during some or all of the period January 1, 2023 to June 30, 2023, business partners of Kolide, Inc. subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Prescient Assurance LLC

DocuSigned by:
John D Wallace
F5ADFA3569EA450...

John D. Wallace, CPA
Chattanooga, TN
September 29, 2023

SECTION 3

System Description

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

Kolide, Inc. (Kolide or the Company) was founded in 2016. There are currently twenty six (26) full-time employees at the time of this writing. The Company is fully remote, with roots in the Boston, MA area and is privately funded.

Kolide's software-as-a-service (SaaS) platform provides endpoint security solutions for teams that value productivity, transparency, and employee happiness. Unlike traditional approaches to endpoint security, Kolide's solution focuses on educating, engaging, and empowering endpoint users to actively participate with their organization's efforts to ensure their devices are meeting organizational guidelines and compliance requirements. Kolide believes that device security starts with the users and provides organizations a collaborative approach between those responsible for ensuring endpoint security and the organization's endpoint users.

The Kolide platform consists of:

- The Kolide SaaS management console that security and network teams utilize to monitor and manage the user endpoints. These are the organization's Kolide administrators. The console provides a drill-down dashboard that provides an overview as well as the detailed drill-down of individual endpoints health and hygiene.
- The Kolide endpoint agent that organization users install on their devices. This agent collects data on the device and transmits the information to the Kolide SaaS management solution.
- Slack integration which is used to communicate endpoint status and issues to both administrators and endpoint users.
- The Kolide console, which provides flexible authentication options, including Single Sign On (SSO) via Google, Slack, Security Assertion Markup Language (SAML), as well as the option for email and password authentication.

Kolide's SaaS product alerts end-users through Slack about security issues or other problems with their device. End-users are given precise instructions on how to fix the problem and can confirm in real-time that the fixes were successfully applied.

DC 2: The Principal Service Commitments and System Requirements

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

Kolide's commitments to users are communicated through Master Service Agreements, online Privacy Policy, and in the description of the service.

Security Commitments

- Security commitments include, but are not limited to, the following:
- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Up time availability of production systems

Confidentiality Commitments

- Confidentiality commitments include, but are not limited to, the following:
- The use of encryption technologies to protect system data both at rest and in transit
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties
- Confidential information must be used only for the purposes explicitly stated in agreements between The Company and user entities

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

The System is comprised of the following components:

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

3.1 Primary Infrastructure

Kolide, Inc. maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner.

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

3.2 Primary Software

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

Primary Software	
System/Application	**Purpose**
PostgreSQL	Transactional database
Redis	Used to maintain cached data
Stripe	Processing payments, storing payment information
Vanta	Compliance monitoring solution
BambooHR	Employee Center for document sharing and on/offboarding procedure
Slack	Real-time collaboration for internal team members & customer communication channels.
Heroku	PaaS, providing all back-end infrastructure, including PostgreSQL database.
GitHub	Code repository and SDLC management.
Checkr	Employee and contractor background check solution
Google Workspace	Email and general Workspace provider. Also manages our mobile MDM.
Asana	Project management tool facilitating communication
Kolide	Kolide uses their own product for internal endpoint management.
Okta	SSO provider and Access Management

Bugsnag	Application error monitoring.
CircleCI	Deployment management and testing.
1Password	Password management tool used by all employees.
Honeycomb	Part of the Kolide eco-system of system monitoring.

3.3 People

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

Kolide, Inc. has a staff of approximately 3 organized in the following functional areas:

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

- CEO - Jason Meller
- VP Sales
- VP Marketing

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

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

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

3.4 Data

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

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

Data is categorized in the following major types of data used by Kolide, Inc.

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

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

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

3.5 Processes and Procedures

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

- Physical Security
- Logical Access
- Availability
- Change Control

- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security

Kolide, Inc.'s production servers are maintained by Heroku. The physical and environmental security protections are the responsibility of Heroku. Kolide, Inc. reviews the attestation reports and performs a risk analysis of Heroku on at least an annual basis.

Logical Access

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

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

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

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

Computer Operations - Backups

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

Computer Operations - Availability

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

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

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

Change Management

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

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

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

Data Communications

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

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

All production code written by Kolide is source-controlled in Git and stored on GitHub as our primary Git remote. As a function of using Github, Kolide is automatically enrolled in GitHub's dependency vulnerability scanning services. This cadence is ongoing and automatic.

Github will produce alerts about vulnerabile javascript and ruby dependencies. Kolide has configured alerting on top of this feature so we are immediately alerted about any critical dependency vulnerabilities.

Engineers are expected to promptly assess and upgrade, remove, and replace vulnerabilities as quickly as possible. Since Github is typically a few days behind other sources of truth for vulnerabilities, engineers are expected to launch an RCA request (Root-cause analysis) to identify the gap in our vulnerability notification visibility.

Boundaries of the System

The boundaries of the Kolide 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 Kolide.

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

DC 4: Disclosures About Identified Security Incidents

No significant incidents have occurred during the audit observation period or interim period since last review.

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

5.1 Integrity and Ethical Values

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

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

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

5.2 Commitment to Competence

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

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

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

5.3 Management's Philosophy and Operating Style

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

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

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

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

5.4 Organizational Structure and Assignment of Authority and Responsibility

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

Kolide, Inc.'s assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

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

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

5.5 HR Policies and Practices

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

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

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

5.6 Risk Assessment Process

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

5.7 Integration with risk assessment

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

5.8 Information and Communication Systems

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

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

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

5.9 Monitoring Controls

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

5.9.1 On-going Monitoring

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

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

Reporting Deficiencies

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

DC 6: Complementary User Entity Controls (CUECs)

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

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

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

DC 7: Complementary Subservice Organization Controls

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

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

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

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

Heroku

Category	Criteria	Control
Security	CC 6.4	Only authorized personnel have access to the facilities housing the system.
Security	CC 6.4	Badge access control systems are in place in order to access the facilities.
Security	CC 6.4	Visitor access to the corporate facility and data center are recorded in visitor access logs
Security	CC 6.4	Visitors are required to wear a visitor badge while onsite at the facilities.
Security	CC 6.4	Visitors are required to check in with security and show a government issued ID prior to being granted access to the facilities
Security	CC 6.4	Visitors are required to have an escort at all times.

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

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

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

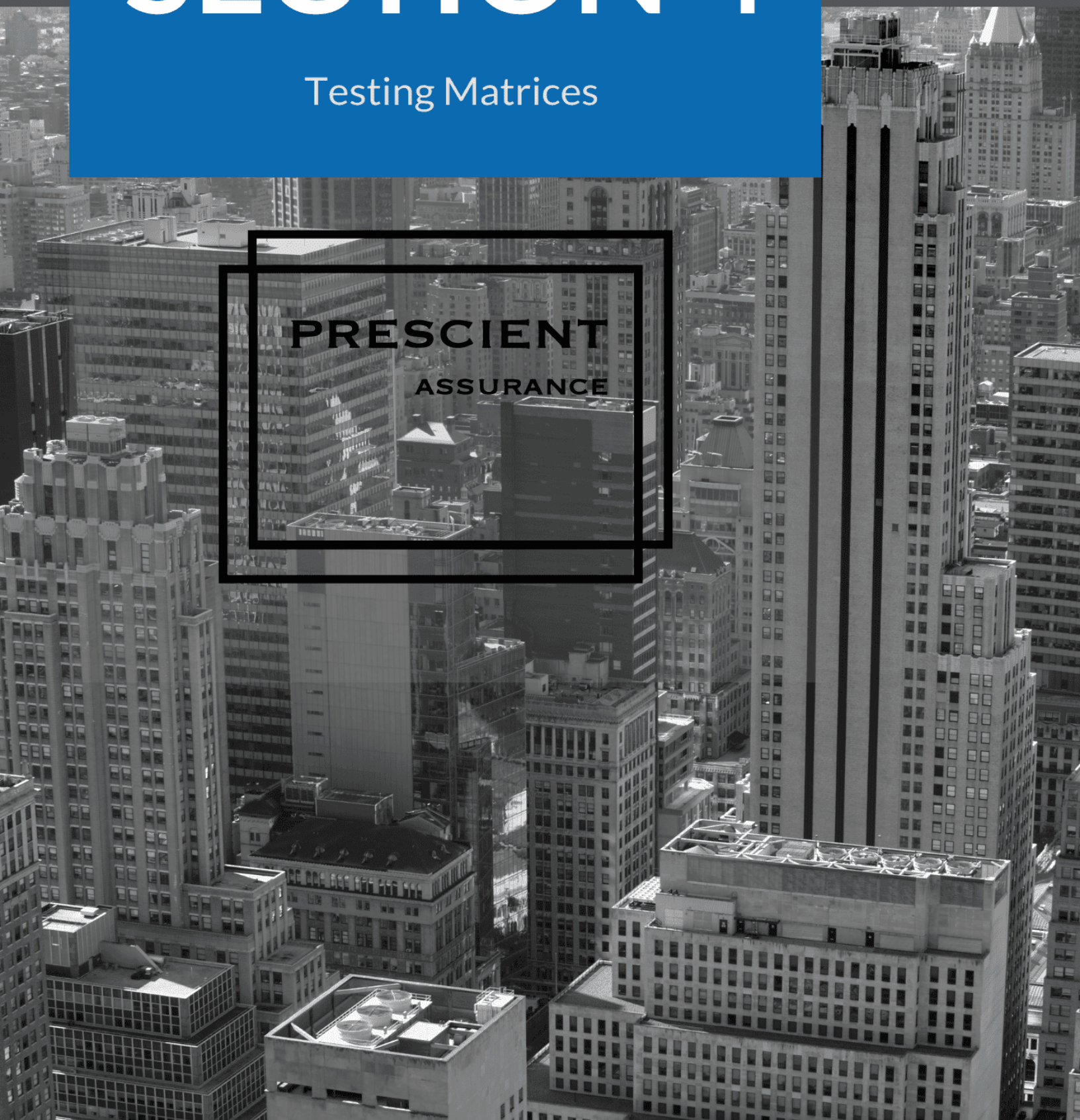
All Common Criteria/Security and Confidentiality criteria were applicable to the Kolide, Inc.'s Kolide system.

DC 9: Disclosures of Significant Changes in Last 1 Year

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

SECTION 4

Testing Matrices



Tests of Operating Effectiveness and Results of Tests

Scope of Testing

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

Prescient Assurance LLC conducted the examination testing throughout the period January 1, 2023 to June 30, 2023.

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

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

Types of Tests Generally Performed

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

Test Types	Description of Tests
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.

Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: • Examination/Inspection of source documentation and authorizations to verify transactions processed. • Examination/Inspection of documents or records for evidence of performance, such as existence of initials or signatures. • Examination/Inspection of systems documentation, configurations, and settings; and • Examination/Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.
Observation	Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Re-performance	Re-performed the control to verify the design and/or operation of the control activity as performed if applicable.

General Sampling Methodology

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

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

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

Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, many times per day	At least 25	At least 40

Manual control, daily (Note 1)	At least 25	At least 40
Manual control, weekly	At least 5	At least 10
Manual control, monthly	At least 3	At least 4
Manual control, quarterly	At least 2	At least 2
Manual control, annually	Test annually	Test annually
Application controls	Test one operation of each relevant aspect of each application control if supported by effective IT general controls; otherwise test at least 15	Test one operation of each application control if supported by effective IT general controls; otherwise test at least 25
IT general controls	Follow guidance above for manual and automated aspects of IT general controls	Follow guidance above for manual and automated aspects of IT general controls
Notes: Some controls might be performed frequently, but less than daily. For such controls, the sample size should be interpolated using the above guidance. Generally, for controls where the number of occurrences ranges from 50 to 250 during the year, our minimum sample size using the above table should be approximately 10% of the number of occurrences.		

Reliability of Information Provided by the Service Organization

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

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices.

Any phrase other than this constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the Operating Effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

Trust ID	COSO Principle	Control Description	Test Applied by the Service Auditor	Test Results
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments.	Inspected the Data Management Policy to determine that the company has established a framework for classifying data based on its sensitivity, value and criticality to ensure that sensitive corporate and customer data can be secured appropriately.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the Access Control Policy to determine that all personnel are required to have a unique user identifier for system access. Inspected the data to determine that all assigned SSH keys are unique, all employees have unique email accounts, No user account has a policy attached directly and the company uses Heroku built-in feature to determine that unique accounts and SSH keys are required to access systems and applications.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the Data Management Policy to determine that the company has established a data classification scheme and handling procedures for relevant data.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the	The company has formal retention and disposal procedures in place to	Inspected the Data Management Policy to determine that internal data retention and disposal procedures have	No exceptions noted.

	entity's objectives related to confidentiality.	guide the secure retention and disposal of company and customer data.	been established stating that the company is required to retain data as long as the company has a need for its use. Additionally, the policy defines the retention periods of various data types. When information is no longer valid or necessary, it should be completely and permanently destroyed.	
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the Third-Party Management Policy to determine that the company requires agreements to be signed with vendors to acknowledge their confidentiality, integrity, availability, and privacy commitments. Inspected the Salesforce Main Services Agreement to determine that the company maintains formal vendor agreements that document their data protection and security commitments. Inspected the company's Privacy Policy and Terms of Service to determine that privacy, information security, and service commitments have been communicated to vendors. through the website.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected the Codiga dashboard showing the confirmation of an account deletion request to determine that the company purges or removes customer data containing confidential information from the application environment in accordance with best practices when customers leave the service.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inspected the Asset Management Policy to determine that the company requires data to be erased prior to disposal or re-use, using an approved technology in order to ensure that data is not recoverable and a certificate of destruction (COD) should be obtained for devices destroyed by a third-party service. Inspected a sample certificate of destruction of a disposed media to determine that the company has electronic media containing confidential information purged or destroyed in accordance with best practices and certificates of	No exceptions noted. No exceptions noted.

			destruction are issued for each device destroyed. Observed that there were no media device disposals that occurred during the observation period.	No performance.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.	Inspected the Human Resource Security Policy to determine that the company performs background checks on new employees. Inspected the personnel records to determine that background checks have been completed for all personnel in the observation period who require them.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the Human Resource Security Policy to determine that the company requires all employees to undergo competence assessments and evaluations at least annually. Inspected a screenshot of employee's evaluation report completed during the observation window to determine that the company performs employee performance evaluations annually.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the Code of Conduct to determine that the company requires its employees to abide by the Code of Conduct in all business matters. Inspected the Human Resource Security Policy to determine that a disciplinary process for violating the company's security policies has been documented. Inspected the policy acceptance data to determine that all new employees have acknowledged the Code of Conduct Policy.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected the Human Resource Security Policy to determine that the company requires its employees to sign a confidentiality or non-disclosure agreement stating the responsibilities for information security. Inspected an employment agreement template, which includes a confidentiality clause, to determine that the company requires employees to sign a confidentiality agreement during onboarding.	No exceptions noted.

			Observed that the company maintains multi-state agreements for hiring new employees.	
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the Code of Conduct to determine that all contractors are required to comply with its terms in all business matters. Inspected the policy acceptance records to determine that the personnel hired during the observation period accepted the Code of Conduct. Inspected a signed contractor agreement dated November 23, 2022, between Kolide Inc. and Gnar Company Inc., which requires the contractor to act in accordance with the relevant laws to determine that contractors agree to act in lawful ways while providing services to the company.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected the Human Resource Security Policy to determine that the company requires its service providers to sign a confidentiality or non-disclosure agreement stating the responsibilities for information security. Inspected the policy acceptance records to determine that the personnel hired during the observation period accepted the Code of Conduct. Inspected a signed contractor agreement dated November 23, 2022, between Kolide Inc. and Gnar Company Inc., to determine that the company requires contractors to sign a confidentiality agreement at the time of engagement. Observed that there were no contractors hired during the observation period.	No exceptions noted. No exceptions noted. No exceptions noted. No performance.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	Observed a screenshot of an Invitation of a Board of Directors meeting on Zoom to determine that the company's board of directors or a relevant subcommittee is briefed by senior management at least annually. Observed the board meeting slides from June 2023 to determine that the	No exceptions noted.

			board meets at least annually to discuss a variety of topics.	
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the LinkedIn profiles of the board members, including the CEO and independent observer, showing their experiences, skills, and qualifications to determine that the board of directors has adequate expertise to oversee responsibilities for internal control.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.	Inspected the LinkedIn profiles of the board members, including the CEO and independent observer, showing their experiences, skills, and qualifications to determine that the board of directors has adequate expertise to lead the management team and oversee the company's internal controls.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	Observed a screenshot of an Invitation of a Board of Directors meeting on Zoom to determine that the company's board of directors or a relevant subcommittee is briefed by senior management at least annually. Observed the board meeting slides from June 2023 to determine that the board meets at least annually to discuss a variety of topics. Inspected the LinkedIn profiles of the board members to determine that the board includes directors that are independent of the company.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the LinkedIn profiles of the board members, including the CEO and independent observer, showing their experiences, skills, and qualifications to determine that the board of directors has adequate expertise to oversee responsibilities for internal control.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy to determine that the company management has defined the roles and responsibilities of the CEO, Director of Operations, Principal Engineer and Executive leadership to oversee the	No exceptions noted.

			design and implementation of information security controls.	
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the organizational chart of the company showing the reporting lines and positions of authority to determine that the company has a formal organizational chart in place that is accessible to internal personnel.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of CEO, Director of Operations, Engineers, Executive leadership, system owners, employees, and contractors for the design, development, implementation, and monitoring of security controls have been defined.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company performs background checks on new employees.	Inspected the Human Resource Security Policy to determine that the company performs background checks on new employees. Inspected the personnel records to determine that background checks have been completed for all personnel in the observation period who require them.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the Human Resource Security Policy to determine that all relevant employees are required to complete security awareness training at the time of hire and annually after that. Observed the onboarding checklists of 2 persons hired during the observation window showing their security awareness training completion dates to determine that on-hire security awareness training was completed at the time of hire.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the Human Resource Security Policy to determine that the company requires all employees to undergo competence assessments and evaluations at least annually. Inspected a screenshot of employee's evaluation report completed during the observation window to determine that the company performs employee performance evaluations annually.	No exceptions noted.

CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of CEO, Director of Operations, Engineers, Executive leadership, system owners, employees, and contractors for the design, development, implementation, and monitoring of security controls have been defined.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the Code of Conduct to determine that the company requires its employees to abide by the Code of Conduct in all business matters. Inspected the Human Resource Security Policy to determine that a disciplinary process for violating the company's security policies has been documented. Inspected the policy acceptance data to determine that all new employees have acknowledged the Code of Conduct Policy.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of CEO, Director of Operations, Engineers, Executive leadership, system owners, employees, and contractors for the design, development, implementation, and monitoring of security controls have been defined.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the Human Resource Security Policy to determine that the company requires all employees to undergo competence assessments and evaluations at least annually. Inspected a screenshot of employee's evaluation report completed during the observation window to determine that the company performs employee performance evaluations annually.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating	Observed that the company uses Vanta for continuous self-assessment and monitoring of internal controls.	No exceptions noted.

		effectively. Corrective actions are taken based on relevant findings.		
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the Operations Security Policy to determine that the company is required to log and monitor all events related to user activities, exceptions, faults, and information security to achieve its security and monitoring objectives. Inspected the list of linked infrastructures to determine that the BambooHR, Github, Google Workspace, AWS, Jira, Heroku, and Slack infrastructures are linked to Vanta. Observed that User activity and API use is tracked in Heroku. Inspected a report of Vanta issues which shows issues and their remediation by configuring a Heroku log drain that stores logs for at least 365 days.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Operations Security Policy to determine that the company requires vulnerability scans to be performed on public-facing systems in the production environment at least quarterly. Inspected the computer inventory to determine that employee computers are monitored with the Vanta agent. Observed that all high, low , medium and critical vulnerabilities identified in packages are addressed in Github. Observed that records of security issues are being tracked in Github. Inspected a quarterly vulnerability scan report to determine that Heroku performs vulnerability scans.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the Human Resource Security Policy to determine that all relevant employees are required to complete security awareness training at the time of hire and annually after that. Observed the onboarding checklists of 2 persons hired during the observation	No exceptions noted.

			window showing their security awareness training completion dates to determine that on-hire security awareness training was completed at the time of hire.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company communicates system changes to authorized inte rnal users.	Inspected the Operations Security Policy to determine that the company requires all system changes to be communicated to relevant internal stakeholders. Observed the screenshot of Slack that shows the communication between the company members regarding system changes to determine that the company uses Slack to communicate system changes to authorized internal users/stakeholders.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Inspected the Information Security Policy to determine that employees are required to report known or suspected security events to the provided email address (panic@kolide.com). The email address is provided for team members to use in situations that require an immediate security response.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Human Resource Security Policy to determine that the management is required to ensure that the policies and procedures have been reviewed annually. Observed that the Access Control Policy, Incident Response Plan, Information Security Policy, and other policies have been reviewed in May 2023 to determine that the company has established information security policies and reviews them annually.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, document, and communicate security and data privacy incidents have been documented.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support	The company provides a description of its products and services to internal and external users.	Inspected the architecture diagram to determine that the company provides a description of its networking components and workflow to internal users.	No exceptions noted.

	the functioning of internal control.		Inspected the company's help page which shows features, articles and FAQ to determine that a description of products and services has been provided to external users.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of CEO, Director of Operations, Engineers, Executive leadership, system owners, employees, and contractors for the design, development, implementation, and monitoring of security controls have been defined.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy to determine that the company management has defined the roles and responsibilities of the CEO, Director of Operations, Principal Engineer and Executive leadership to oversee the design and implementation of information security controls.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the help guide of the company's products and solutions on its website to determine that Smartcat provides guidelines related to system operations. Inspected the company's website to determine that a support system and an email address (support@kolide.com) have been provided to customers for external support.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company notifies customers of critical system changes that may affect their processing.	Inspected the Operations Security Policy to determine that the company is required to inform customers about changes to the systems. Inspected the company's release notes on the company's website to determine that system changes are communicated to all customers through the website. Observed the product's details on the company's website to determine that the company communicates any changes or new product launches on its website.	No exceptions noted.

CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected the information security program on the company's website to determine that the security methodologies implemented by the company have been communicated to customers and other users. Inspected the Terms of Service and Privacy Policy to determine that service and privacy commitments have been described to all users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Inspected the architecture diagram to determine that the company provides a description of its networking components and workflow to internal users. Inspected the company's help page which shows features, articles and FAQ to determine that a description of products and services has been provided to external users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the company's website to determine that a support system and an email address (support@kolide.com) have been provided to users to report issues, complaints, and other concerns.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the Third-Party Management Policy to determine that the company requires agreements to be signed with vendors to acknowledge their confidentiality, integrity, availability, and privacy commitments. Inspected the Salesforce Main Services Agreement to determine that the company maintains formal vendor agreements that document their data protection and security commitments. Inspected the company's Privacy Policy and Terms of Service to determine that privacy, information security, and service commitments have been communicated to vendors. through the website.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the	The company has a documented risk management program in place that includes	Inspected the Risk Management Policy to determine that the risk management processes along with risk response and treatment strategies have been	No exceptions noted.

	identification and assessment of risks relating to objectives.	guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	documented to identify, resolve, and document risks.	
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Management Policy to determine that the risk management processes along with risk response and treatment strategies have been documented that help the company achieve its business objectives. Inspected the risk register, which shows risk scenarios, scores, treatment plans, and approvers to determine that the company is required to identify and mitigate risks that hinder the achievement of its business objectives.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the plan is to be tested at least annually. Observed records of a BC/DR plan tabletop exercise that was designed to facilitate communication among select personnel regarding the implementation of recovery operations at Kolide following an event causing the outage of mission critical systems. It was designed to improve the readiness of Kolide's team and help validate existing Business Continuity and Disaster Recovery Plan procedures.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third-Party Management Policy to determine that the third-party risk management, security standards, and vendors' service review and monitoring requirements have been described. Observed that the company creates and manages a vendor inventory. Inspected the vendor directory to determine that the company has compliance security reports for critical vendors and reviews them annually.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity	The company's risk assessments are performed at least	Inspected the Risk Management Policy to determine that the company is required to perform a formal IT risk	No exceptions noted.

	and analyzes risks as a basis for determining how the risks should be managed.	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.	assessment at least annually. Inspected the risk assessment data, which includes the risk register, which shows risk scenarios, scores, treatment plans, and approvers to determine that the company performs risk assessments annually. Additionally, the risk assessment includes a consideration of the potential for fraud	
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the risk management processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the Risk Management Policy to determine that the company is required to perform a formal IT risk assessment at least annually. Inspected the risk assessment data, which includes the risk register, which shows risk scenarios, scores, treatment plans, and approvers to determine that the company performs risk assessments annually. Additionally, the risk assessment includes a consideration of the potential for fraud	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and	Inspected the Risk Management Policy to determine that the risk management processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks.	No exceptions noted.

		mitigation strategies for those risks.		
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the Penetration Test Report from February 2023, which shows the tools used for the penetration test, the result of the test, and the detail of publicly available information, to determine that the company performs penetration tests annually. Observed the screenshot of the communication regarding vulnerabilities found during the penetration test and the actions that the company intends to take regarding the vulnerabilities.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the Operations Security Policy to determine that a change management process has been documented stating the stages of planning, testing, approving, communicating, and documenting changes. Inspected the code deployment/release process in Github to determine that a CI/CD system is in use and that changes are documented and deployed consistently.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the Risk Management Policy to determine that the company is required to perform a formal IT risk assessment at least annually. Inspected the risk assessment data, which includes the risk register, which shows risk scenarios, scores, treatment plans, and approvers to determine that the company performs risk assessments annually. Additionally, the risk assessment includes a consideration of the potential for fraud	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks	Inspected the Risk Management Policy to determine that the risk management processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks.	No exceptions noted.

		associated with the identified threats, and mitigation strategies for those risks.		
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the Penetration Test Report from February 2023, which shows the tools used for the penetration test, the result of the test, and the detail of publicly available information, to determine that the company performs penetration tests annually. Observed the screenshot of the communication regarding vulnerabilities found during the penetration test and the actions that the company intends to take regarding the vulnerabilities.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third-Party Management Policy to determine that the third-party risk management, security standards, and vendors' service review and monitoring requirements have been described. Observed that the company creates and manages a vendor inventory. Inspected the vendor directory to determine that the company has compliance security reports for critical vendors and reviews them annually.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Observed that the company uses Vanta for continuous self-assessment and monitoring of internal controls.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Operations Security Policy to determine that the company requires vulnerability scans to be performed on public-facing systems in the production environment at least quarterly. Inspected the computer inventory to determine that employee computers are monitored with the Vanta agent. Observed that all high, low, medium and critical vulnerabilities identified in packages are addressed in Github.	No exceptions noted.

			Observed that records of security issues are being tracked in Github. Inspected a quarterly vulnerability scan report to determine that Heroku performs vulnerability scans.	
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Observed that the company uses Vanta for continuous self-assessment and monitoring of internal controls.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third-Party Management Policy to determine that the third-party risk management, security standards, and vendors' service review and monitoring requirements have been described. Observed that the company creates and manages a vendor inventory. Inspected the vendor directory to determine that the company has compliance security reports for critical vendors and reviews them annually.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the risk management processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Human Resource Security Policy to determine that the management is required to ensure that the policies and procedures have been reviewed annually. Observed that the Access Control Policy, Incident Response Plan, Information Security Policy, and other policies have been reviewed in May 2023 to determine that the company	No exceptions noted.

			has established information security policies and reviews them annually.	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Human Resource Security Policy to determine that the management is required to ensure that the policies and procedures have been reviewed annually. Observed that the Access Control Policy, Incident Response Plan, Information Security Policy, and other policies have been reviewed in May 2023 to determine that the company has established information security policies and reviews them annually.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Operations Security Policy to determine that the company has described secure system engineering principles, change control procedures, and secure development guidelines.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy to determine that the company has established access control procedures, including access provisioning, de-provisioning, access change, and review procedures. Observed a screenshot showing various points of access that were provisioned to an employee during the observation window.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Operations Security Policy to determine that the company has described secure system engineering principles, change control procedures, and secure development guidelines.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is	The company's information security policies and procedures are	Inspected the Human Resource Security Policy to determine that the management is required to ensure that	No exceptions noted.

	expected and in procedures that put policies into action.	documented and reviewed at least annually.	the policies and procedures have been reviewed annually. Observed that the Access Control Policy, Incident Response Plan, Information Security Policy, and other policies have been reviewed in May 2023 to determine that the company has established information security policies and reviews them annually.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the Third-Party Management Policy to determine that the third-party risk management, security standards, and vendors' service review and monitoring requirements have been described. Observed that the company creates and manages a vendor inventory. Inspected the vendor directory to determine that the company has compliance security reports for critical vendors and reviews them annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, document, and communicate security and data privacy incidents have been documented.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Management Policy to determine that the risk management processes along with risk response and treatment strategies have been documented that help the company achieve its business objectives. Inspected the risk register, which shows risk scenarios, scores, treatment plans, and approvers to determine that the company is required to identify and mitigate risks that hinder the achievement of its business objectives.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Operations Security Policy and Business Continuity and Disaster Recovery Plan to determine that information backup requirements have been documented stating that Kolide infrastructure personnel are required to test the accuracy of all Customer data backup systems and the efficacy and timeliness of the restoration process annually.	No exceptions noted.

CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to determine that internal data retention and disposal procedures have been established stating that the company is required to retain data as long as the company has a need for its use. Additionally, the policy defines the retention periods of various data types. When information is no longer valid or necessary, it should be completely and permanently destroyed.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the risk management processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that the responsibilities of CEO, Director of Operations, Engineers, Executive leadership, system owners, employees, and contractors for the design, development, implementation, and monitoring of security controls have been defined.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the Operations Security Policy to determine that a change management process has been documented stating the stages of planning, testing, approving, communicating, and documenting changes. Inspected the change review data to determine that at least one approval is required to merge the changes to the default branch for all linked AWS repositories and the visibility of all repositories has been set to private. Inspected the code deployment/ release process in GitLab to determine that a CI/CD system is in use and that	No exceptions noted.

			changes are documented and deployed consistently.	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Access Control Policy to determine that the company is required to grant access to users for systems and applications according to the principle of least privilege. Inspected the data to determine that all SSH keys assigned to users are unique, SSL/TLS is enabled on the admin page of the Heroku console and all Heroku accounts have password policies enabled to determine that production network authentication is enforced.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.	Inspected the Access Control Policy to determine that the company is required to use Multi-Factor Authentication (MFA) to enforce unique production system authentication. Inspected a list of accounts and MFA status to determine that all Heroku, Okta, Google Workspace and GitHub accounts have MFA enabled for managing database access through authentication.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to databases to authorized users with a business need.	Inspected the Access Control Policy to determine that the company is required to grant access to users for systems and applications according to the principle of least privilege. Inspected the data to determine that all Heroku and Github accounts have been linked to users within Vanta.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the application to authorized users with a business need.	Inspected the Access Control Policy to determine that the company grants users access to company systems and applications based on the principle of least privilege. Observed the screenshot that shows that the verification is necessary for the access to the Okta infrastructure. Inspected the data to determine that all AWS accounts have been linked to users within Vanta. Inspected a list of accounts and MFA status to determine that all Heroku, Okta, Google Workspace and GitHub	No exceptions noted.

			accounts have MFA enabled for managing database access through authentication.	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the Access Control Policy to determine that the company is required to give privileged access to users based on the principle of least privilege. Observed the records to determine that the company uses the built-in firewall feature of Heroku. Observed the records to determine that only authorized employees are assigned unique SSH keys to determine that access to firewalls is restricted to authorized personnel with a business need and SSH keys. Observed the records to determine that SSH is required for server access, Public SSH is denied and unwanted traffic is filtered via Heroku.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the operating system to authorized users with a business need.	Inspected the Access Control Policy to determine that the company grants users access to company systems and applications based on the principle of least privilege. Inspected the personnel data to determine that all Heroku accounts have been linked to users within Vanta.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the Cryptography Policy to determine that access to keys and secrets is to be tightly controlled in accordance with the Access Control Policy. Observed the record to determine that the infrastructure provider's key management was used.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's datastores housing sensitive customer data are encrypted at rest.	Inspected the Cryptography Policy to determine that the company is required to implement cryptographic controls to mitigate data risks. Inspected the data to determine that all Heroku databases are encrypted at rest to determine that the company	No exceptions noted.

			encrypts data stores containing sensitive customer data.	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy to determine that the company has established access control procedures, including access provisioning, de-provisioning, access change, and review procedures. Observed a screenshot showing various points of access that were provisioned to an employee during the observation window.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the Access Control Policy to determine that all personnel are required to have a unique user identifier for system access. Inspected the data to determine that all assigned SSH keys are unique, all employees have unique email accounts, No user account has a policy attached directly and the company uses Heroku built-in feature to determine that unique accounts and SSH keys are required to access systems and applications.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the Access Control Policy to determine that the company requires remote connections to all its production systems and networks to be encrypted. Inspected the security certificate of the website, which is valid until October 22, 2023, to determine that the website is secured using an encrypted connection. Observed the record to determine that SSL/TLS is enabled on the company website.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the production network to authorized users with a business need.	Inspected the Access Control Policy to determine that the company grants users access to company systems and applications based on the principle of least privilege. Inspected the personnel data to determine that all Heroku accounts have been linked to users within Vanta.	No exceptions noted.

CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company maintains a formal inventory of production system assets.	Inspected the Asset Management Policy to determine that all assets are required to be stored in an inventory owned by a specific individual or group. Inspected the asset inventory to determine that the company maintains an inventory of Heroku resources, GitHub repositories, and computers managed with the Vanta agent. Observed the record to determine that the asset inventory tracks resources that contain user data.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the Access Control Policy to determine that the company has documented the requirements for password length and complexity. Inspected the computer inventory to determine that all computers managed with the Vanta agent have a password manager installed and all Okta accounts have password policies enabled.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the personnel directory to determine that MFA is enabled on all Heroku, Okta, Google Workspace and GitHub user accounts.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the Data Management Policy to determine that the company has established a data classification scheme and handling procedures for relevant data.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts access to migrate changes to production to authorized personnel.	Inspected the Operations Security Policy to determine that ADRs are proposed to the mono-repo through a Github Pull Request and discussed through the standard Github Flow process until agreed upon and merged. Inspected the data to determine that at least one approval is required to merge to the default branch for all linked GitHub repositories and at least one repository in the linked version control system has been updated in the last 30 days, visibility of all repositories has been set to private and invitation	No exceptions noted.

			to the company aren't older than 1 year to determine that approval and access are required to migrate changes to the main branch.	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the network architecture diagram displaying workflow details to determine that the company's network is segmented to prevent unauthorized access to customer data.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the Access Control Policy to determine that the company requires all access and rights modification requests to be documented in an access request ticket or email and approval is required from the system or data owner, or management. Inspected the access request made via an internal communication channel displaying details of access to be granted to determine that access requests are documented and required formal approval.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Access Control Policy to determine that the company is required to grant access to users for systems and applications according to the principle of least privilege. Inspected the data to determine that all SSH keys assigned to users are unique, SSL/TLS is enabled on the admin page of the Heroku console and all Heroku accounts have password policies enabled to determine that production network authentication is enforced.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy to determine that the company has established access control procedures, including access provisioning, de-provisioning, access change, and review procedures. Observed a screenshot showing various points of access that were provisioned to an employee during the observation window.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting	The company ensures that user access to in-scope	Inspected the Access Control Policy to determine that the company requires	No exceptions noted.

	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.	system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	all access and rights modification requests to be documented in an access request ticket or email and approval is required from the system or data owner, or management. Inspected the access request made via an internal communication channel displaying details of access to be granted to determine that access requests are documented and required formal approval.	
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the Access Control Policy to determine that the company is required to revoke the access privileges of terminated employees within 08 business hours. Observed several termination checklists displaying the list of accounts removed to determine that the company uses a checklist to revoke access of the employees who have left the company.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company conducts access reviews at least annually for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the Access Control Policy to determine that the company requires administrators to perform access rights reviews of users, administrators, and service accounts on at least an annual basis. Inspected two quarterly access review tickets to determine that access reviews are performed. Inspected the list of linked accounts to determine that all GitHub, Okta, G Suite Admin, Jira, Heroku, BambooHR, Slack and Customercheckr are linked to Vanta to determine that access activity is tracked through Vanta.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the Access Control Policy to determine that the company requires all access and rights modification requests to be documented in an access request ticket or email and approval is required from the system or data owner, or management. Inspected the access request made via an internal communication channel displaying details of access to be granted to determine that access	No exceptions noted.

			requests are documented and required formal approval.	
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Access Control Policy to determine that the company is required to grant access to users for systems and applications according to the principle of least privilege. Inspected the data to determine that all SSH keys assigned to users are unique, SSL/TLS is enabled on the admin page of the Heroku console and all Heroku accounts have password policies enabled to determine that production network authentication is enforced.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the Access Control Policy to determine that the company is required to revoke the access privileges of terminated employees within 08 business hours. Observed several termination checklists displaying the list of accounts removed to determine that the company uses a checklist to revoke access of the employees who have left the company.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company conducts access reviews at least annually for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the Access Control Policy to determine that the company requires administrators to perform access rights reviews of users, administrators, and service accounts on at least an annual basis. Inspected two quarterly access review tickets to determine that access reviews are performed. Inspected the list of linked accounts to determine that all GitHub, Okta, G Suite Admin, Jira, Heroku, BambooHR, Slack and Customercheckr are linked to Vanta to determine that access activity is tracked through Vanta.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy to determine that the company has established access control procedures, including access provisioning, de-provisioning, access change, and review procedures. Observed a screenshot showing various points of access that were provisioned	No exceptions noted.

	and segregation of duties, to meet the entity's objectives.		to an employee during the observation window.	
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company conducts access reviews at least annually for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the Access Control Policy to determine that the company requires administrators to perform access rights reviews of users, administrators, and service accounts on at least an annual basis. Inspected two quarterly access review tickets to determine that access reviews are performed. Inspected the list of linked accounts to determine that all GitHub, Okta, G Suite Admin, Jira, Heroku, BambooHR, Slack and Customercheckr are linked to Vanta to determine that access activity is tracked through Vanta.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the Access Control Policy to determine that the company is required to revoke the access privileges of terminated employees within 08 business hours. Observed several termination checklists displaying the list of accounts removed to determine that the company uses a checklist to revoke access of the employees who have left the company.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to determine that internal data retention and disposal procedures have been established stating that the company is required to retain data as long as the company has a need for its use. Additionally, the policy defines the retention periods of various data types. When information is no longer valid or necessary, it should be completely and permanently destroyed.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected the Codiga dashboard showing the confirmation of an account deletion request to determine that the company purges or removes customer data containing confidential information from the application environment in accordance with best practices when customers leave the service.	No exceptions noted.
CC6.5	The entity discontinues logical and physical	The company has electronic media	Inspected the Asset Management Policy to determine that the company	No exceptions noted.

	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.	containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	requires data to be erased prior to disposal or re-use, using an approved technology in order to ensure that data is not recoverable and a certificate of destruction (COD) should be obtained for devices destroyed by a third-party service. Inspected a sample certificate of destruction of a disposed media to determine that the company has electronic media containing confidential information purged or destroyed in accordance with best practices and certificates of destruction are issued for each device destroyed. Observed that there were no media device disposals that occurred during the observation period.	No exceptions noted. No performance.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the Information Security Policy to determine that for confidential data in-transit, care is required to be taken to ensure all communications that could be surveilled are encrypted using industry standard transport encryption. Observed that SSL/TLS is configured on the admin page of Heroku console. Inspected the security certificate of the website which is valid until October 21, 2023, to determine that the company's website has an unexpired and valid certificate that only accepts TLS connections using up-to-date cipher suites, and redirects HTTP to HTTPS via a 3XX status code.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the personnel directory to determine that MFA is enabled on all Heroku, Okta, Google Workspace and GitHub user accounts.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected the Incident Response Plan to determine that the company is required to use a firewall for blocking unauthorized connection attempts. Observed that the company uses the built-in firewall features of Heroku, so	No exceptions noted.

			the responsibility for reviewing the firewall rules lies with Heroku.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses firewalls and configures them to prevent unauthorized access.	Inspected the Incident Response Plan to determine that the company is required to use a firewall for blocking unauthorized connection attempts. Observed that the company uses the built-in firewall features of Heroku.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the Operations Security Policy to determine that the company uses Heroku's built-in monitoring so that operations and engineering receive timely notifications when error rates on web applications reach an unacceptable threshold. Observed that the company uses Heroku for infrastructure management and system patch monitoring. Inspected the security issue tracking data to determine that all GitHub tasks are labeled with a security tag. Inspected the security issue resolution data to determine that all relevant GitHub tasks labeled with a security tag are marked as complete. Inspected a resolved Jira ticket to determine that identified vulnerabilities are resolved in a timely manner.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Access Control Policy to determine that the company is required to grant access to users for systems and applications according to the principle of least privilege. Inspected the data to determine that all SSH keys assigned to users are unique, SSL/TLS is enabled on the admin page of the Heroku console and all Heroku accounts have password policies enabled to determine that production network authentication is enforced.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's network and system hardening standards are documented, based on industry best practices,	Observed that the company uses the built-in firewall features of Heroku. Therefore, Heroku is responsible for the review of the firewall as well as the network and system hardening standards.	No exceptions noted.

		and reviewed at least annually.	Inspected the Operations Security Policy to determine that the company reviews the core-values and standards of the Engineering organization, along with the processes they maintain to ensure and uphold these values and rigid standards.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the Operations Security Policy to determine that the company uses Heroku's built-in monitoring so that operations and engineering receive timely notifications when error rates on web applications reach an unacceptable threshold. Inspected the users' data to determine that several employees have the Vanta Agent installed on their workstations. Observed that the company uses Heroku for infrastructure management and that user activity and API use is tracked in Heroku.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the Access Control Policy to determine that the company requires remote connections to all its production systems and networks to be encrypted. Inspected the security certificate of the website, which is valid until October 22, 2023, to determine that the website is secured using an encrypted connection. Observed the record to determine that SSL/TLS is enabled on the company website.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company encrypts portable and removable media devices when used.	Inspected the Information Security Policy to determine that the company requires removable media use for valid business purposes to be encrypted. Inspected the devices' data to determine that all employee workstations with the Vanta Agent installed have encrypted hard drives.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the Information Security Policy to determine that for confidential data in-transit, care is required to be taken to ensure all communications that could be surveilled are encrypted using industry	No exceptions noted.

	transmission, movement, or removal to meet the entity's objectives.		standard transport encryption. Observed that SSL/TLS is configured on the admin page of Heroku console. Inspected the security certificate of the website which is valid until October 21, 2023, to determine that the company's website has an unexpired and valid certificate that only accepts TLS connections using up-to-date cipher suites, and redirects HTTP to HTTPS via a 3XX status code.	
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Observed that the company uses Vanta as an MDM solution.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the Operations Security Policy to determine that the company uses Heroku's built-in monitoring so that operations and engineering receive timely notifications when error rates on web applications reach an unacceptable threshold. Observed that the company uses Heroku for infrastructure management and system patch monitoring. Inspected the security issue tracking data to determine that all GitHub tasks are labeled with a security tag. Inspected the security issue resolution data to determine that all relevant GitHub tasks labeled with a security tag are marked as complete. Inspected a resolved Jira ticket to determine that identified vulnerabilities are resolved in a timely manner.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency	Inspected the Operations Security Policy to determine that the company has described secure system engineering principles, change control procedures, and secure development guidelines.	No exceptions noted.

		changes), and maintenance of information systems and related technology requirements.		
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected the devices' data to determine that an employee Windows workstation managed with the Vanta Agent has antivirus software installed. Inspected the users' data to determine that in-scope employees have the Vanta Agent installed on their workstations.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Operations Security Policy to determine that the company requires vulnerability scans to be performed on public-facing systems in the production environment at least quarterly. Inspected the computer inventory to determine that employee computers are monitored with the Vanta agent. Observed that all high, low , medium and critical vulnerabilities identified in packages are addressed in Github. Observed that records of security issues are being tracked in Github. Inspected a quarterly vulnerability scan report to determine that Heroku performs vulnerability scans.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the Operations Security Policy to determine that vulnerability management and scanning procedures have been documented. Moreover, the policy states that the company uses Heroku's built-in monitoring so that operations and engineering receive timely notifications when error rates on web applications reach an unacceptable threshold.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being	Inspected the Operations Security Policy to determine that a change management process has been documented stating the stages of planning, testing, approving, communicating, and documenting changes. Inspected the change review data to	No exceptions noted.

		implemented in the production environment.	determine that at least one approval is required to merge the changes to the default branch for all linked AWS repositories and the visibility of all repositories has been set to private. Inspected the code deployment/ release process in GitLab to determine that a CI/CD system is in use and that changes are documented and deployed consistently.	
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the Risk Management Policy to determine that the company is required to perform a formal IT risk assessment at least annually. Inspected the risk assessment data, which includes the risk register, which shows risk scenarios, scores, treatment plans, and approvers to determine that the company performs risk assessments annually. Additionally, the risk assessment includes a consideration of the potential for fraud	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the Operations Security Policy to determine that a change management process has been documented stating the stages of planning, testing, approving, communicating, and documenting changes. Inspected the code deployment/release process in Github to determine that a CI/CD system is in use and that changes are documented and deployed consistently.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the Operations Security Policy to determine that vulnerability management and scanning procedures have been documented. Moreover, the policy states that the company uses Heroku's built-in monitoring so that operations and engineering receive timely notifications when error rates on web applications reach an unacceptable threshold.	No exceptions noted.

CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the Operations Security Policy to determine that the company uses Heroku's built-in monitoring so that operations and engineering receive timely notifications when error rates on web applications reach an unacceptable threshold. Observed that the company uses Heroku for infrastructure management.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the Operations Security Policy to determine that the company uses Heroku's built-in monitoring so that operations and engineering receive timely notifications when error rates on web applications reach an unacceptable threshold. Observed that the company uses Heroku for infrastructure management and system patch monitoring. Inspected the security issue tracking data to determine that all GitHub tasks are labeled with a security tag. Inspected the security issue resolution data to determine that all relevant GitHub tasks labeled with a security tag are marked as complete. Inspected a resolved Jira ticket to determine that identified vulnerabilities are resolved in a timely manner.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the Operations Security Policy to determine that the company is required to log and monitor all events related to user activities, exceptions, faults, and information security to achieve its security and monitoring objectives. Inspected the list of linked infrastructures to determine that the BambooHR, GitHub, Google Workspace, AWS, Jira, Heroku, and Slack infrastructures are linked to Vanta. Observed that User activity and API use is tracked in Heroku.	No exceptions noted.

			Inspected a report of Vanta issues which shows issues and their remediation by configuring a Heroku log drain that stores logs for at least 365 days.	
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Operations Security Policy to determine that the company requires vulnerability scans to be performed on public-facing systems in the production environment at least quarterly. Inspected the computer inventory to determine that employee computers are monitored with the Vanta agent. Observed that all high, low, medium and critical vulnerabilities identified in packages are addressed in Github. Observed that records of security issues are being tracked in GitHub. Inspected a quarterly vulnerability scan report to determine that Heroku performs vulnerability scans.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the Operations Security Policy to determine that the company uses Heroku's built-in monitoring so that operations and engineering receive timely notifications when error rates on web applications reach an unacceptable threshold. Inspected the users' data to determine that several employees have the Vanta Agent installed on their workstations. Observed that the company uses Heroku for infrastructure management and that user activity and API use is tracked in Heroku.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the Penetration Test Report from February 2023, which shows the tools used for the penetration test, the result of the test, and the detail of publicly available information, to determine that the company performs penetration tests annually. Observed the screenshot of the communication regarding vulnerabilities found during the penetration test and the actions that	No exceptions noted.

			the company intends to take regarding the vulnerabilities.	
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, document, and communicate security and data privacy incidents have been documented.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the Incident Response Plan to determine that incident reporting procedures along with incident categories, classification, and communication have been defined. Inspected the security issue resolution data to determine that all relevant GitHub tasks labeled with a security tag are marked as complete.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the Operations Security Policy to determine that the company uses Heroku's built-in monitoring so that operations and engineering receive timely notifications when error rates on web applications reach an unacceptable threshold. Observed that the company uses Heroku for infrastructure management and system patch monitoring. Inspected the security issue tracking data to determine that all GitHub tasks are labeled with a security tag. Inspected the security issue resolution data to determine that all relevant GitHub tasks labeled with a security tag are marked as complete. Inspected a resolved Jira ticket to determine that identified vulnerabilities are resolved in a timely manner.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company tests their incident response plan at least annually.	Inspected the Incident Response Plan from February 2023 to determine that the company performs annual exercises to test their incident response plan.	No exceptions noted.

CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the Incident Response Plan to determine that incident reporting procedures along with incident categories, classification, and communication have been defined. Inspected the security issue resolution data to determine that all relevant GitHub tasks labeled with a security tag are marked as complete.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, document, and communicate security and data privacy incidents have been documented.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Operations Security Policy to determine that the company requires vulnerability scans to be performed on public-facing systems in the production environment at least quarterly. Inspected the computer inventory to determine that employee computers are monitored with the Vanta agent. Observed that all high, low , medium and critical vulnerabilities identified in packages are addressed in Github. Observed that records of security issues are being tracked in GitHub. Inspected a quarterly vulnerability scan report to determine that Heroku performs vulnerability scans.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the plan is to be tested at least annually. Observed records of a BC/DR plan tabletop exercise that was designed to facilitate communication among select personnel regarding the implementation of recovery operations at Kolide following an event causing the outage of mission critical systems. It was designed to improve the readiness of Kolide's team and help	No exceptions noted.

			validate existing Business Continuity and Disaster Recovery Plan procedures.	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the incident response procedure and roles and responsibilities of response team members to report, resolve, document, and communicate security and data privacy incidents have been documented.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company tests their incident response plan at least annually.	Inspected the Incident Response Plan from February 2023 to determine that the company performs annual exercises to test their incident response plan.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the Incident Response Plan to determine that incident reporting procedures along with incident categories, classification, and communication have been defined. Inspected the security issue resolution data to determine that all relevant GitHub tasks labeled with a security tag are marked as complete.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the Operations Security Policy to determine that a change management process has been documented stating the stages of planning, testing, approving, communicating, and documenting changes. Inspected the change review data to determine that at least one approval is required to merge the changes to the default branch for all linked AWS repositories and the visibility of all repositories has been set to private. Inspected the code deployment/ release process in GitLab to determine that a CI/CD system is in use and that changes are documented and deployed consistently.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are	Inspected the Operations Security Policy to determine that the company uses Heroku's built-in monitoring so that operations and engineering receive timely notifications when error rates on web applications reach an unacceptable threshold. Observed that the company uses Heroku for infrastructure management	No exceptions noted.

		hardened against security threats.	and system patch monitoring. Inspected the security issue tracking data to determine that all GitHub tasks are labeled with a security tag. Inspected the security issue resolution data to determine that all relevant GitHub tasks labeled with a security tag are marked as complete. Inspected a resolved Jira ticket to determine that identified vulnerabilities are resolved in a timely manner.	
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Operations Security Policy to determine that the company requires vulnerability scans to be performed on public-facing systems in the production environment at least quarterly. Inspected the computer inventory to determine that employee computers are monitored with the Vanta agent. Observed that all high, low, medium and critical vulnerabilities identified in packages are addressed in Github. Observed that records of security issues are being tracked in Github. Inspected a quarterly vulnerability scan report to determine that Heroku performs vulnerability scans.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company restricts access to migrate changes to production to authorized personnel.	Inspected the Operations Security Policy to determine that ADRs are proposed to the mono-repo through a Github Pull Request and discussed through the standard Github Flow process until agreed upon and merged. Inspected the data to determine that at least one approval is required to merge to the default branch for all linked GitHub repositories and at least one repository in the linked version control system has been updated in the last 30 days, visibility of all repositories has been set to private and invitation to the company aren't older than 1 year to determine that approval and access	No exceptions noted.

			are required to migrate changes to the main branch.	
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Operations Security Policy to determine that the company has described secure system engineering principles, change control procedures, and secure development guidelines.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Observed that the company uses the built-in firewall features of Heroku. Therefore, Heroku is responsible for the review of the firewall as well as the network and system hardening standards. Inspected the Operations Security Policy to determine that the company reviews the core-values and standards of the Engineering organization, along with the processes they maintain to ensure and uphold these values and rigid standards.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the Penetration Test Report from February 2023, which shows the tools used for the penetration test, the result of the test, and the detail of publicly available information, to determine that the company performs penetration tests annually. Observed the screenshot of the communication regarding vulnerabilities found during the penetration test and the actions that the company intends to take regarding the vulnerabilities.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that the risk management processes along with risk response and treatment strategies have been documented to identify, resolve, and document risks.	No exceptions noted.

CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the Risk Management Policy to determine that the company is required to perform a formal IT risk assessment at least annually. Inspected the risk assessment data, which includes the risk register, which shows risk scenarios, scores, treatment plans, and approvers to determine that the company performs risk assessments annually. Additionally, the risk assessment includes a consideration of the potential for fraud	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Observed the company's cyber insurance policy valid until July 2024 to determine that the company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the communications and escalation plan with roles and responsibilities of key personnel and business continuity strategies for critical services have been described.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the Third-Party Management Policy to determine that the company requires agreements to be signed with vendors to acknowledge their confidentiality, integrity, availability, and privacy commitments. Inspected the Salesforce Main Services Agreement to determine that the company maintains formal vendor agreements that document their data protection and security commitments. Inspected the company's Privacy Policy and Terms of Service to determine that privacy, information security, and service commitments have been communicated to vendors. through the website.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with	The company has a vendor management program in	Inspected the Third-Party Management Policy to determine that the third-	No exceptions noted.

	vendors and business partners.	place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	party risk management, security standards, and vendors' service review and monitoring requirements have been described. Observed that the company creates and manages a vendor inventory. Inspected the vendor directory to determine that the company has compliance security reports for critical vendors and reviews them annually.	