SOC 2 Type 2 Report

Iterative Inc.

April 17, 2023 to July 17, 2023
Next Report Issue Date: September 1, 2024

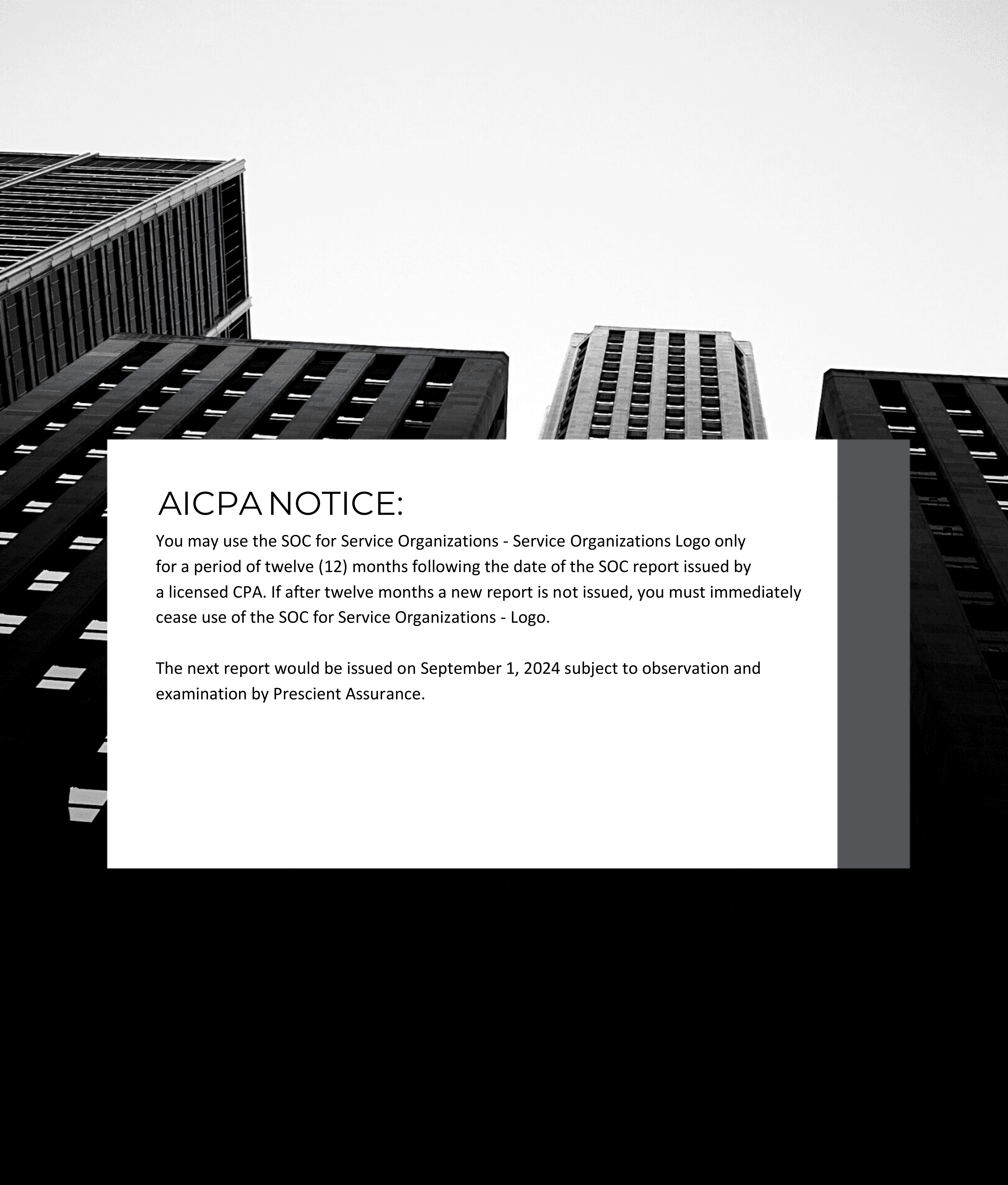
A Type 2 Independent Service Auditor's Report on Controls Relevant to Security, Confidentiality, and Availability

AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

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

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

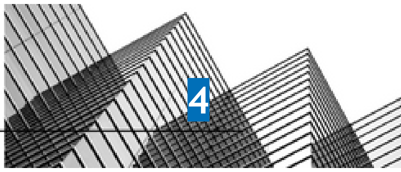


AICPA NOTICE:

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 1, 2024 subject to observation and examination by Prescient Assurance.

Table of Contents



SECTION 1

Management's Assertion

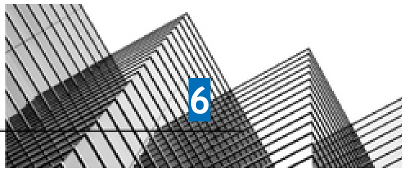
iterative

Management’s Assertion

We have prepared the accompanying description of Iterative Inc.’s system throughout the period April 17, 2023 to July 17, 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 users with information about Iterative Inc.’s system that may be useful when assessing the risks arising from interactions with Iterative Inc.’s system, particularly information about system controls that Iterative 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, Confidentiality, and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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



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

a. The description presents Iterative Inc.’s system that was designed and implemented throughout the period April 17, 2023 to July 17, 2023 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period April 17, 2023 to July 17, 2023, to provide reasonable assurance that Iterative 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 Iterative Inc.’s controls during that period.
c. The controls stated in the description operated effectively throughout the period April 17, 2023, to July 17, 2023, to provide reasonable assurance that Iterative 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 Iterative Inc.’s controls operated effectively throughout the period.

DocuSigned by:
Kenneth Thom
7928326C6574490...

Kenneth Thom
Director of Operations
Iterative Inc.

SECTION 2

Independent Service Auditor's Report

PRESCIENT
ASSURANCE

Independent Service Auditor's Report

To: Iterative Inc.

Scope

We have examined Iterative Inc.'s ("Iterative Inc.") accompanying description of its Iterative Studio SAAS product system found in Section 3, titled Iterative Inc. System Description throughout the period April 17, 2023, to July 17, 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 April 17, 2023, to July 17, 2023, to provide reasonable assurance that Iterative Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

Iterative 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 Iterative Inc.'s service commitments and system requirements were achieved. In Section 1, Iterative Inc. has provided the accompanying assertion titled "Management's Assertion of Iterative Inc." (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Iterative 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.

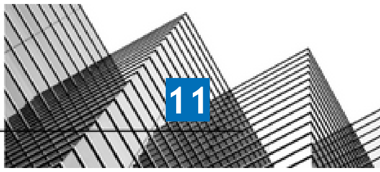
Inherent Limitations

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 Iterative Inc.’s system that was designed and implemented throughout the period April 17, 2023, to July 17, 2023, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period April 17, 2023, to July 17, 2023, to provide reasonable assurance that Iterative 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 Iterative Inc.’s controls throughout the period.
c. The controls stated in the description operated effectively throughout the period April 17, 2023, to July 17, 2023, to provide reasonable assurance that Iterative 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 Iterative Inc.’s controls operated effectively throughout the period.



Restricted Use

This report is intended solely for the information and use of Iterative Inc., user entities of Iterative Inc.'s system during some or all of the period April 17, 2023 to July 17, 2023, business partners of Iterative 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:

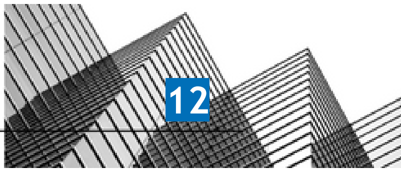
1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
3. Internal control and its limitations.
4. Complementary subservice organization controls and how 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

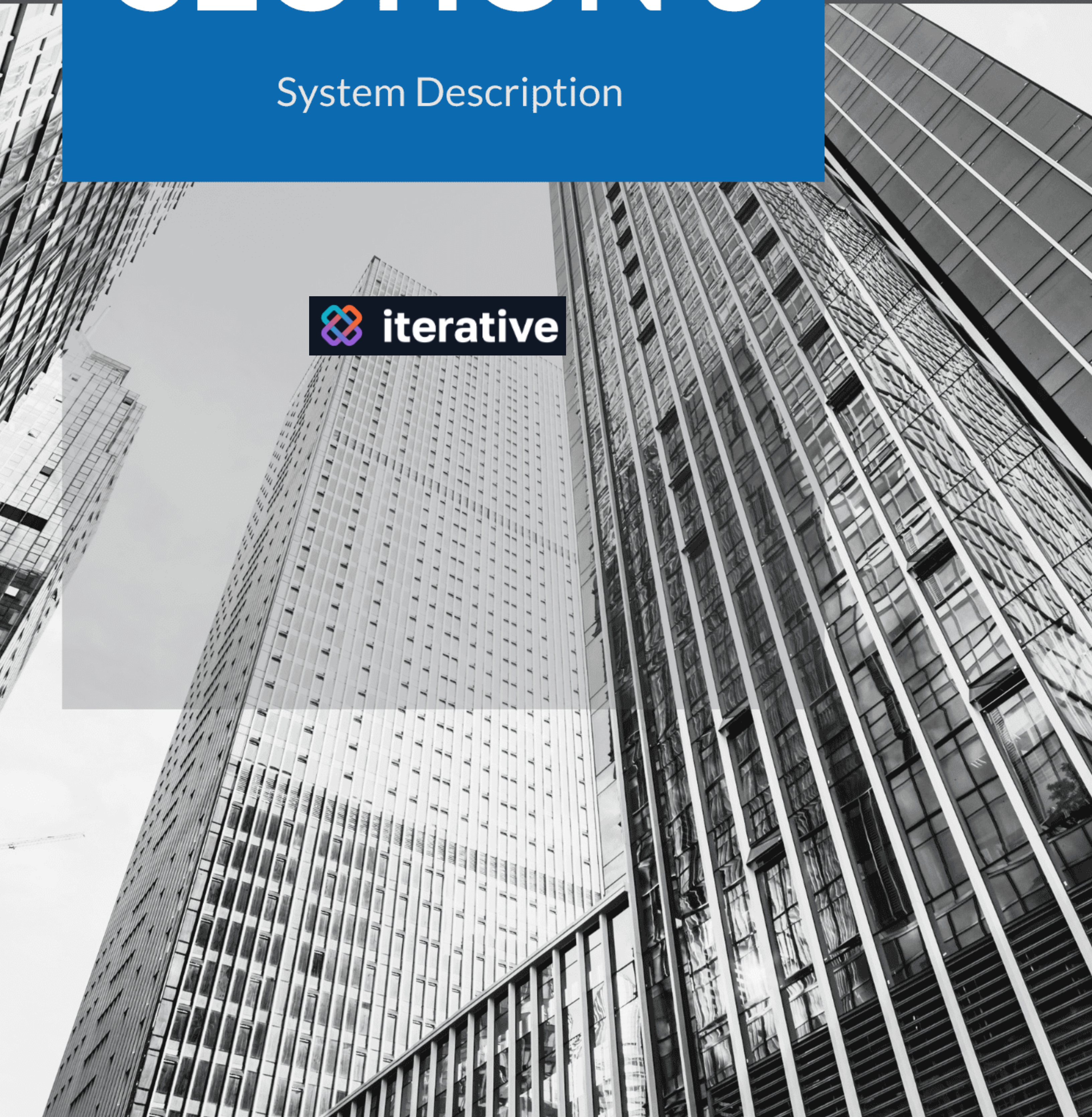
DocuSigned by:
John D Wallace
F5ADFA3569EA450...

John D. Wallace, CPA
Chattanooga, TN
September 1, 2023



SECTION 3

System Description



iterative

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

Company background: Iterative incorporated in 2018, initially offering open-source tools for ML engineers and data scientists (DVC, CML). We launched our first enterprise SaaS product, Studio, in 2021. Iterative raised a Series A round of $20M in Q2 2021.

About Us: https://iterative.ai/about

Studio: https://studio.iterative.ai

LinkedIn: https://www.linkedin.com/company/iterative-ai/

DC 2: The Principal Service Commitments and System Requirements

Principal Service commitments:

- See pricing page: https://iterative.ai/pricing
- Studio docs: https://dvc.org/doc/studio

Trust Service Criteria:

- Security and Privacy: https://iterative.ai/security-and-privacy
- Privacy policy: https://iterative.notion.site/Privacy-Cookie-Policy-edbce9b3b3d14f26950b7dca617b2033

System Requirements:

Supported browsers - ES6 support required

Major browsers support matrix:

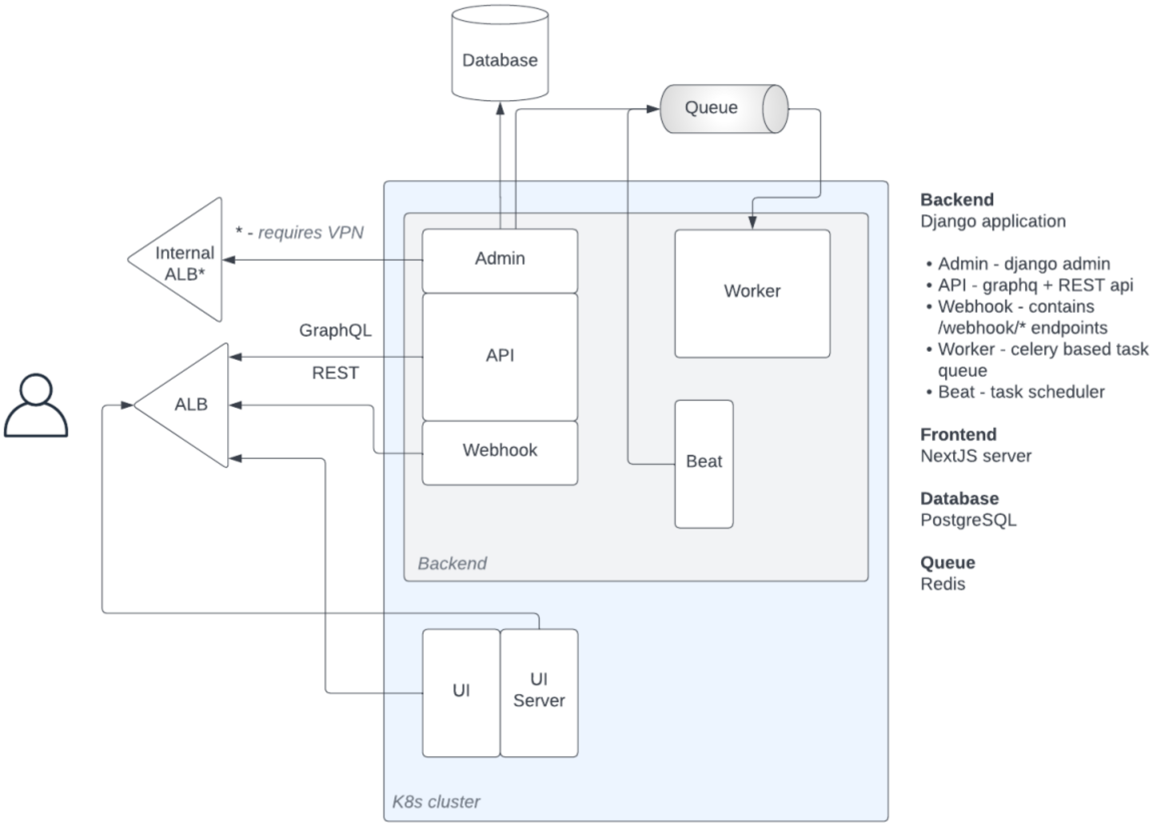
Browser	Minimal version
Chrome	63
Firefox	67
Edge	16
Safari	11.1
Opera	48
Android browser	104

- RAM - we recommend at least 4GB of RAM on client machine for a smooth experience in studio

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

3.1 Primary Infrastructure

System Diagrams



Backend
Django application

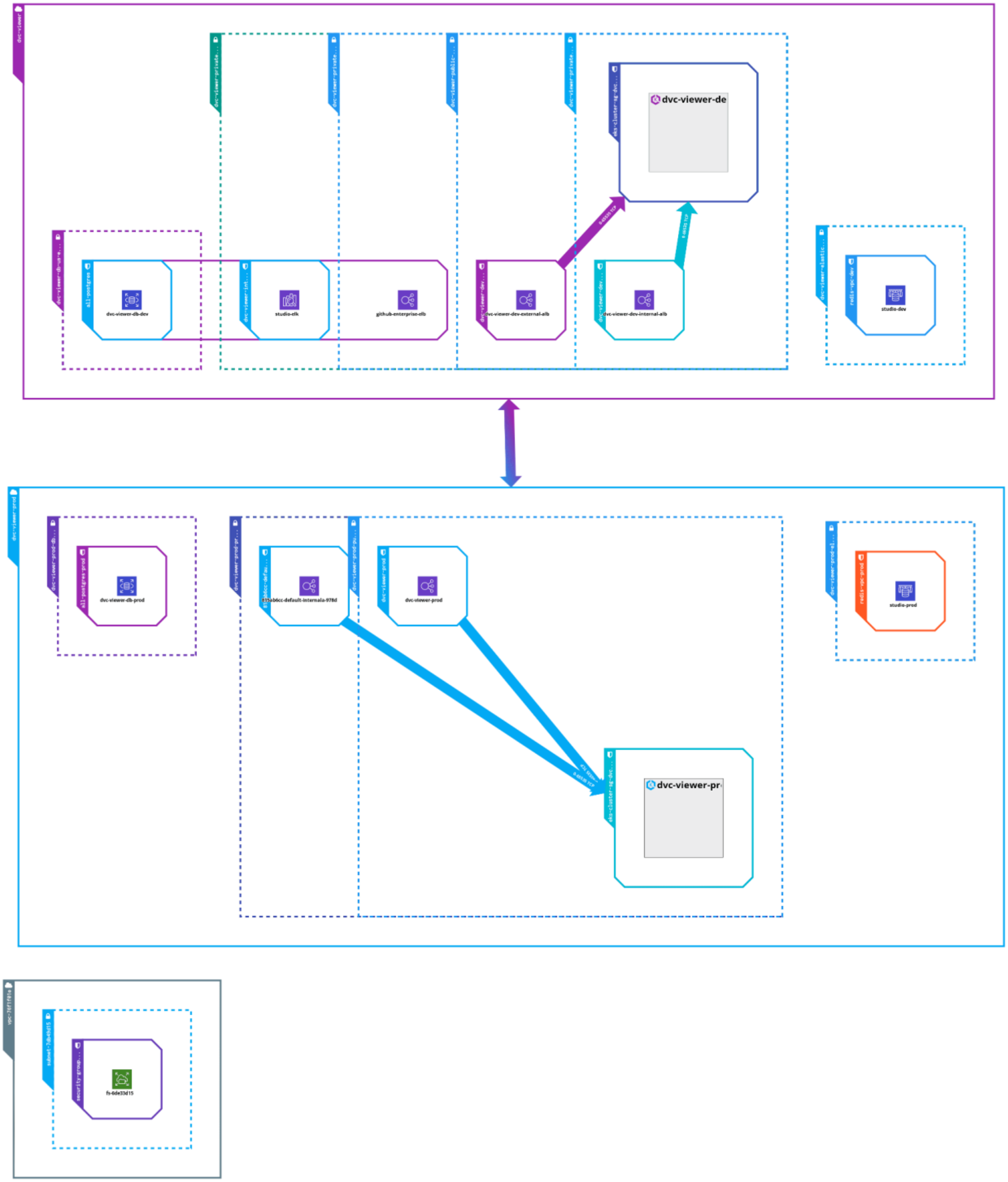
- Admin - django admin
- API - graphq + REST api
- Webhook - contains /webhook/* endpoints
- Worker - celery based task queue
- Beat - task scheduler

Frontend
NextJS server

Database
PostgreSQL

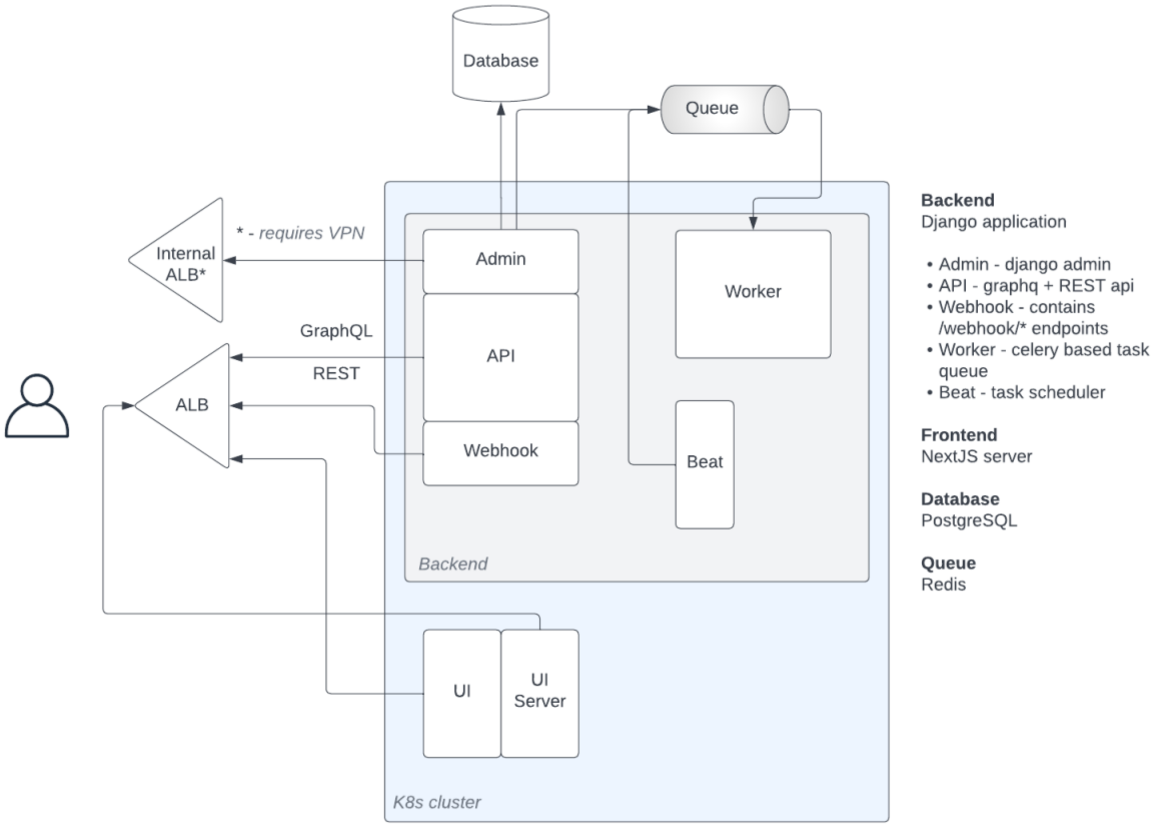
Queue
Redis

Cloudcraft Network Diagram


dvc-viewer
dvc-viewer-private...
dvc-viewer-private...
dvc-viewer-public-...
dvc-viewer-private...
eks-cluster-sg-dvc...
dvc-viewer-de
dvc-viewer-db-us-e...
all-postgres
dvc-viewer-db-dev
dvc-viewer-int...
studio-elk
github-enterprise-elb
dvc-viewer-dev...
dvc-viewer-dev-external-alb
0-65535 TCP
dvc-viewer-dev...
dvc-viewer-dev-internal-alb
0-65535 TCP
dvc-viewer-elastic...
redis-vpc-dev
studio-dev
dvc-viewer-prod
dvc-viewer-prod-db...
all-postgres-prod
dvc-viewer-db-prod
dvc-viewer-prod-pr...
835ab6cc-defau...
835ab6cc-default-internala-978d
dvc-viewer-prod-pu...
dvc-viewer-prod
dvc-viewer-prod
0-65535 TCP
eks-cluster-sg-dvc...
dvc-viewer-pr
dvc-viewer-prod-el...
redis-vpc-prod
studio-prod
vpc-76f1f01e
security-group...
fs-6de33d15

3.2 Primary Software

We use many managed services - so the system diagram is also relevant to our SW stack



Backend
Django application

- Admin - django admin
- API - graphq + REST api
- Webhook - contains /webhook/* endpoints
- Worker - celery based task queue
- Beat - task scheduler

Frontend
NextJS server

Database
PostgreSQL

Queue
Redis

Tech Stack:

- Backend: Python, Django, dockerized, Celery workers
- Frontend: Typescript, React, Redux, dockerized
- API Scheme: GraphQL, Rest
- Primary DB: RDS (AWS managed postgres)
- Caching DB: Redis
- CI/CD: Python, terraform, ArgoCD, GH Actions
- Analytics: Plausible, Mixpanel
  Alerting: Sentry
- DNS/cloudfront - Cloudflare
- Logging stack: ES, Kibana, AWS Cloudwatch

3.3 People

Full Org chart can be found in rippling: https://app.rippling.com/employee-list/orgchart

Studio Team - Development:

- Manager: Ivan Shcheklein (CTO)
- Manager: Oded Messer (Director of Engineering)
    - Sviatlana Sachkouskaya - SW Engineer (Frontend)
    - Maksim Shmakov - SW Engineer (Frontend)
    - Jelle Bouwman - SW Engineer (Frontend)
    - Fam (Thomas) Kumwar - SW Engineer (Frontend)
    - Ranjit (Amrit) Ghimire - SW Engineer (Backend)
    - Ivan Longin - SW Engineer (Backend)
    - Jesper Svendsen - SW Engineer (Platform / Infra)
    - Marcin Jasion - SW Engineer (Platform / Infra)
- Manager: Dmitry Petrov (CEO)
    - Tapa Dipti Sitaula - Senior Product Engineer

Sales/CSE Teams:

- Manager: Dmitry Petrov (CEO):
    - Jervis Hui - Director, operations, Go To Market
    - Michael (Mike) Moynihan - Sales
    - Mikhail Rozhkov - Solution Engineer
    - Tibor Mach - Solution Engineer

3.4 Security Processes and Procedures

3.4.1 Secure Development and Maintenance

Development activities contain safe guards and control to maintain a high level of security as a routine:

- Developer attention to development and testing best practices
- Continuous automation for security scanning - identifying and alerting on vulnerabilities both on supply chain (dependencies) and by coding patterns (static code scanning).
- Periodic external penetration testing and DAST (yearly, last done july 2023).
- Internal Security team to be consulted with on every possible finding, risk and mitigation strategies
- A bug bounty program - to encourage safe disclosure by independent security researchers. Those findings are discussed and addressed internally with high priority.

3.4.2 Securing the Development Environment

Access to the development environment is restricted only to authorized employees via logical access control. Development, testing, and production environments are logically separated and access to them is enforced.

3.4.3 Secure Engineering Principles

Oded Messer issues procedures for secure information system engineering, both for the development of new systems and for the maintenance of the existing systems, as well as set the minimum-security standards which must be complied with.

The same secure engineering principles are applied to outsourced development.

3.4.4 Security Requirements

When acquiring new information systems or developing or changing existing ones, the appropriate project team must document the applicable security requirements.

3.4.5 Security Requirements Related to Public Networks

Oded Messer is responsible for defining security controls related to information in application services passing over public networks:

- the description of authentication systems to be used
- the description of how confidentiality and integrity of information is to be ensured
- the description of how non-repudiation of actions will be ensured

Oded Messer is responsible for defining controls for online transactions, which must include the following:

- how misrouting will be prevented
- how incomplete data transmission will be prevented
- how unauthorized message alteration will be prevented
- how unauthorized message duplication will be prevented
- how unauthorized data disclosure will be prevented

3.4.6 Checking and Testing the Implementation of Security Requirements

Oded Messer is responsible for defining the methodology, responsibilities and the timing of checking whether all specified security requirements have been met, and whether the system is acceptable for production.

3.4.7 Repository and Version Control

Iterative utilizes code version control management tools to track and manage code development, testing, and merges with production. Only employees with a business need have access to code version control management tools based on the principle of least privilege.

3.4.8 Change Control

Changes in the development and during the maintenance of the systems must be done according to the Change Management Policy.

3.4.9 Protection of Test Data

Confidential and restricted data, as well as data that can be related to individual persons must not be used as test data. Exceptions may be approved only by Oded Messer, in which case Oded Messer must define how such test data are protected.

3.4.10 Required Security Training

Oded Messer defines the level of security skills and knowledge required for the development process. All engineers must review the OWASP Top 10 as defined in the Change Management Policy.

3.5 Data

- Main flow for user data is simple:
    - Git forge (github, gitlab, bitbucket) -> Studio app (parsed in memory, cached on local Redis) -> RDS (AWS, isolated network)
- Some user auxiliary user data (plots, charts) is fetched from user provided storage (e.g. S3, Azure storage, GCS storage) and cached on a company owned S3 bucket (blobvault) for display purposes. The data is not processed, shared, transferred in any capacity or for any other purpose.

3.6 Third Party Access

Key Vendors for Studio app (more comprehensive list on secureframe)

- Github
- Gitlab
- Bitbucket
- S3
- Google Drive
- AWS (EKS, RDS, ELB, CloudTrail logs, ES)
- Sentry.io
- Mixpanel
- Plausible
- 1password - internal password management
- Notion - proposals, docs
- Slack - IM, operations

3.7 System Boundaries

- Studio - SaaS App (Integrates with some other company open source tools and /or their metadata via picking up git commits/files/tags)
- DVC - FOSS
- CML - FOSS
- GTO - FOSS
- MLEM - FOSS

DC 4: Disclosures about Identified Security Incidents

No incidents identified / disclosed as of date.

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

5.1 Integrity and Ethical Values

Equal Opportunity Employment

Iterative is an equal opportunity employer. We thrive on diversity and are committed to creating an inclusive environment for all Team Members.

Professionalism

All employees must show integrity and professionalism in the workplace.

Job Duties and Authority

All Team Members should fulfill their job duties with integrity and respect toward customers, stakeholders and the community. Supervisors and managers must not abuse their authority.

We encourage mentorship throughout Iterative.

Communication and Collaboration

All Team Members should be responsive and open for communication with their colleagues, supervisors or team members. Employees should be friendly and collaborative. They should try not to disrupt the workplace or present obstacles to their colleagues' work.

Benefits

Iterative expects employees to not abuse their employment benefits.

Compliance with Law

Team Members must comply with all applicable laws including environmental, safety and fair dealing laws. We expect everyone to be ethical and responsible during Iterative business dealings.

Conflict of Interest

Conflicts of interest occur when an employee, contractor, or job applicant's personal interests may not align with company needs or interests. We expect you to avoid any personal, financial, or other interests that might hinder your capability or willingness to perform your job duties. If you believe that a conflict may occur, please contact your manager immediately.

- Types of conflicts of interest may include:
- Personal investments
- Outside employment, advisory roles, board seats, and starting your own business Business opportunities found through work
- Inventions
- Accepting gifts, entertainment, and other business courtesies

Anti Corruption

Iterative Employees & partners are prohibited from authorizing, making, offering, promising, requesting, receiving or accepting bribes or kickbacks in any form. This prohibition applies to all forms of bribery, including commercial bribery as well as bribery of government employees or officials.

The Anti-Corruption Laws prohibiting bribery are very broad, so that many kinds of gifts or entertainment provided to government employees or officials might be considered improper. For that reason, Team Members and Partners may not give anything of value to any government employee or official in order to wrongfully influence the government employee or official, obtain or retain business or receive any improper advantage. This prohibition applies regardless of whether the payment or offer of payment is made directly to the government employee or official or indirectly through a third party.

It is critical to understand that, for purposes of the Anti-Corruption Laws, the term "government official" generally includes any employee of a company that is owned or controlled by a government or governmental agency. So, for example, this means that someone working for a telecom, energy company, internet company or hospital in another country that is owned or controlled by that country's government is a "government official".

It is important to avoid even the appearance of impropriety. If you have any questions about whether a payment may be improper or violate this Policy, consult your manager or a director before any payment or offer is made.

Gift, Entertainment, Travel & promotional expenditures

Gifts in the business context can be an appropriate way for business people to display respect for each other. Iterative expects the use of good judgment and moderation when giving or receiving entertainment or gifts.

No gift or entertainment should ever be offered, given, provided or accepted by Team Members/Partners unless it:

- is reasonable and not extravagant ("of token value" - such as shirts or tote bags that reflect Company's business name and/or logo)
- is appropriate under the circumstances and serves a valid business purpose (e.g. swag in a convention)
- is customary and appropriate under U.S. and local customs;
- is not being offered for any improper purpose, and could not be construed as a bribe, kickback or payoff; no explicit or implicit business interaction is conditioned by it.
- does not violate any company policy;

- does not violate any U.S., local or international laws or regulations; and is accurately described in your expense or other reports and Company's books and records (if gift given). It is essential that Team Members and Partners accurately report expenditures for gifts or entertainment so that the purpose, amount, and recipient of the gift are obvious & transparent to personnel in the company. Expense reports should accurately state the purpose of the expenditures and the identities of the individuals receiving the gifts or entertainment and state whether the gift or entertainment was given to a government employee or official.

Significant legal restrictions apply with regard to providing gifts, entertainment, travel and promotional expenditures related to government officials. Team Members and Partners must make sure they fully understand all such restrictions and associated policies and procedures (refer to "Anti corruption" section). In each instance: all gifts, entertainment, or promotional expenses which are intended to induce a government employee or official to misuse their position or to obtain an improper advantage are strictly prohibited, regardless of their value!

Team Members and Partners should avoid even the appearance of impropriety. Any gift or expense that is lavish or might otherwise prove embarrassing for the Company is prohibited. If Team Members and Partners have any question regarding the appropriateness of any gift or expense, they should consult their manager or a director before giving the gift or incurring the expense.

Internet and Social Media

Employees should never share any intellectual property or the status of any of their assignments on social media, with the exception of non-confidential information that can be shared on public support areas to address user and customer support requests.

When representing the company, employees should always be respectful and avoid speaking in specifics about their work. Employees should never post discriminatory, offensive, or other illegal language on social media.

5.2 Commitment to Competence

Performance Reviews

Timely performance reviews will be conducted by managers to ensure high professional standards of all work, adherence to best practices, consistency of work product, alignment with company goals and proper conduct according to company culture.

Eligibility

All employees are provided an annual performance review.

5.3 Management's Philosophy and Operating Style

About Us: https://iterative.ai/about

5.4 Organizational Structure and Assignment of Authority and Responsibility

Operating Model

Iterative started by offering Git-based open source products (DVC, CML) to the ML community. Based on the popularity of these products, Iterative developed a GUI-based SaaS product, Studio, which offers ML teams a collaborative user-friendly solution for seamless data and model management, experiment tracking, visualization and automation.

Job descriptions and roles are defined and assigned based on the specific products Iterative is developing and the business needs of the company as its user numbers, customers and sales grow.

5.5 Human Resource Policies and Practices

Performance Review Schedule

Performance evaluations are conducted annually with specific dates announced by Management. Each manager is responsible for the timely and equitable assessment of the performance and contribution of their team members.

Salary Increases

A performance evaluation does not always result in an automatic salary increase. The employee's overall performance and salary level relative to position responsibilities must be evaluated to determine whether a salary increase is warranted.

Processes

Management will establish the format and timing of all review processes. The reviews may change from year to year and from person to person. The completed evaluations will be retained and documented.

Managers may not discuss any proposed action with the employee until all written approvals are obtained.

Management will review all salary increase/adjustment requests to ensure compliance with company policy and that they fall within the provided guidelines.

5.6 Security Management

Platform team manages information security - cloud accounts, system security and infrastructure.

Permissions for AWS production environments are managed using IaC (terraform) in https://github.com/iterative/itops

System is monitored and logs are retained in ES and retained for 1 year

Best practices are used to monitor network traffic, do security scans, and monitor analytics to ensure the smooth running of the service

Employees in the company go through security training, read all company policies including information and data security and undergo documented onboarding and offboarding procedures. All engineers are security aware and consider security risks and best practices in their d2d work.

5.7 Security and Privacy Policies

Security and Privacy Policy: *https://iterative.ai/security-and-privacy*

5.8 Personnel Security

People Security

Background Check

All Iterative personnel are required to complete a background check. An authorized member of Iterative must review each background check in accordance with local laws.

Confidentiality

Prior to accessing sensitive information, personnel are required to sign an industry-standard confidentiality agreement protecting Iterative confidential information.

Security Awareness Training

Iterative has a security awareness training program in place to promote the understanding of security policies and procedures. All personnel are required to undergo training following initial employment and annually thereafter. Completion of the training program is logged by Iterative.

System Access Security

Iterative adheres to the principle of least privilege, specifying that team members will be given access to only the information and resources necessary to perform their job functions as determined by management or a designee. Requests for escalation of or changes to privilege and access are documented and require approval by an authorized manager. System access is revoked upon termination or resignation.

Account Audits

Audits of access and privileges to sensitive Iterative applications, infrastructure, systems, and data are performed and reviewed by authorized personnel.

Password Security

Unique accounts and passwords are required for all users. Passwords must be kept confidential and not shared with multiple users. Where possible, all user and system accounts must have a minimum of ten characters including alpha (upper and lower case), one numeric and one non-alphanumeric character. All accounts must use unique passwords not used elsewhere.

Rotation Requirements

If a password is suspected to be compromised, the password should be rotated immediately and the security team should be immediately notified.

Storing Passwords

Passwords must only be stored using a Iterative approved password manager. Iterative does not hard code passwords or embed credentials in static code.

Acceptable Use

Ownership

Iterative is the owner of all company-issued hardware and electronic systems and of the data stored in them or transmitted from them.

User Responsibilities

Personnel should not make any discriminatory, disparaging, defamatory or harassing comments when discussing Iterative, using social media, blogging or otherwise engaging in any conduct to the detriment of Iterative.

Personal Use Systems

Incidental use of Iterative electronic systems for personal use is permitted provided such use does not interfere with productivity, confidentiality or the business and is not in conflict with team member responsibilities outlined in any Iterative policy.

Compliance

For security and network maintenance purposes, Iterative may monitor and track system access and content of Iterative hardware, system(s) and information to reasonably ensure compliance with applicable laws, regulations and Iterative policies.

Iterative reserves the right to access and audit any devices, networks and systems to ensure compliance with any Iterative policy.

Remote Work

Any Iterative issued devices used to access company applications, systems, infrastructure, or data must be used only by the authorized employee or contractor of such device.

Employees or contractors accessing the Iterative network or other cloud-based networks or tools are required to use HTTPS/TLS 1.1+ at a minimum to protect data-in-transit.

If you are in a public space, ensure your sight lines are blocked and do not have customer conversations or other confidential conversations. If someone is close to you, assume they can see and hear everything. Connecting directly to a public wireless network that doesn't employ, at minimum, WPA-2 or an equivalent wireless protocol is prohibited.

While working at home, employees and applicable contractors should be mindful when visitors (e.g. maintenance personnel) are at their residences, as visitors could become privy to sensitive information left up on computer screens.

5.9 Physical Security and Environmental Controls

Iterative is a fully remote company with no centralized headquarters or physical network. Because of this, physical and environmental security procedures have been deemed unnecessary. There are specific considerations taken, however, regarding remote work and the security risks inherent specific to companies that are fully remote. These can be found in our BYOD policy, our Business Continuity and Disaster Recovery plan, and our Information Security Policy (AUP) or physical security policy.

5.10 Change Management

Changes are managed and recorded in 3 key systems:

- Github - task management via issues and boards, code change requests (PR)

- Notion - docs, RFC
- Monday - planning (roadmap), task management

All code changes - are reviewed, approved and undergo automated testing (including studio and IT ops) testing includes automatic tests (CI) deployment is done in an automated way using a CD pipelines that deploys to production instances.

5.11 System Monitoring

We use various monitoring and alerting tools and systems; key systems:

- Sentry.io - live alerts from dev/production studio instances and other websites
- Cloudwatch - collecting logs on resources, RDS queries
- AWS Guard - DDoS protection
- AWS guardDuty - malware protection
- Logs - collection by custom code (using fleuntbit) to ES, viewed with Kibana, used for debugging
- Grafana - monitoring infra - EKS clusters, RDS, Redis, ES, ALB
- Plausible + Mixpanel - analytics
- Cloudflare - DNS and web gateway

5.12 Incident Management

The Security Incident Response Plan provides a systematic incident response process for all Information Security Incident(s) (defined below) that affect any of Iterative's information technology systems, network, or data, including Iterative data held or services provided by third-party vendors or other service providers. From time to time, Iterative may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations.

5.13 Data Backup and Recovery

RDS is the only storage service that holds a meaningful state for studio app - backed up daily, easy to restore.

No strong Studio availability SLAs are guaranteed today - RDS is auto-recovering but not fully HA, with plans to move to full HA setup in the future perf need

5.14 System Account Management

onboarding/offboarding is managed and recorded. All permission changes are recorded in dedicated #security-ops slack channel

Critical permissions - AWS, are managed by code.

Vendor access controls are unified in secureframe

Quarterly Access Control review is being held by Engineering: Director + Platform team

5.15 Data Classification

Data classification policy can be found here: https://app.secureframe.com/policies/31a004d0-c493-414a-a32c-75d629704e68

All Iterative data should be classified into one of the following four classifications:

- Restricted Data,
- Confidential Data,
- Internal Data, and
- Public Data.

All data that is not explicitly classified should be treated as confidential data and a classification should be determined and requested.

5.16 Risk Management Responsibilities

Risks are being assessed and analyzed for all new activities, and existing processes are constantly being discussed to improve and mitigate risks.

Risk Assessment and Treatment report will be created for any new significant risk identified or taken.

Oded Messer or a designee is responsible for creating the risk assessment and treatment report and delivering results to senior management and other applicable team members including risk responses and documentation of risks that will be accepted by the organization such as threats or vulnerabilities that will likely impact the organization and with a low impact cost. All risk assessment reports must be documented and retained for a minimum of three years.

Specifically, risks of Legal, HR and Security incidents are mitigated by policies that are in place, and operation risks are mitigated by continuously challenging processes and encouraging key learning, conclusions, and documentation of all key activities.

5.17 Risk Management Program Activities

Risk monitoring - monitoring key changes to product, tech stack, new features implemented or new vendors interfaced with. The functionality, stability of any new tool / package / service are assessed in the exploration phase - those risks include security risks but also operational and work capacity risks.

For Fraud / Security risks:

- Policies are put in place wrt data handling, private information, all employees go through security training covering those subjects upon onboarding (secureframe);
- Company laptops are equipped with Kolide MDM and important irregularities are tracked and remediated (OS updated, firewall, disk encryption, etc);
- Security and integrity scan systems are deployed to monitor production services and alert on abnormalities.

Any key changes / concerns are discussed with the CEO/CTO to try and identify risks to the plan, company, business, culture, etc.

5.18 Integration with Risk Assessment

Multiple engineers are participating in any decisions affecting control and processes, and risk management (security, efficiency) are discussed continuously.

Engineering culture is highly security/risk aware - this is supported by an open engineering culture, engineers self-report incidents and constantly strive to improve standards and systems.

Automated scans and alerting systems are in place for preemptive monitoring

Privacy - We avoid parsing / hosting user data (sans caching). We sanitize logs.

5.19 Information and Communications Systems

Communication and collaboration tools and processes:
Google Workspace, Slack, Github, Notion, Discord, Figma, Miro, Monday.

5.20 Data Communication

Storage EBS volumes, RDS, Redis and ES storage are encrypted with AES-256-GCM keys

K8s Secrets - same

OpenVPN keys use RSA and tls-crypt 2048 bit keys - rotated yearly

We are using TLSv1.2 for encryption in transit both internally for studio<>RDS and external communication

Passwords and keys are stored and shared in the Engineering org via 1password (with different access scope and different vaults) and all critical accounts, like AWS IAM require 2FA.

5.21 Monitoring Controls

Pen-test - currently ongoing (august). Remediation after initial test is WIP, progress can be tracked here: https://github.com/iterative/itops/issues/425 (private repo, requires access, please contact us if relevant)

Kolide - open source MDM (endpoint client) to monitor and alert about dev-box configuration and security discrepancies

Compliance automation - Secureframe - to accumulate and alert about discrepancies with different vendors

DC 6: Complementary User Entity Controls (CUECs)

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

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.

Trust Services Criteria	Complementary User Entity Controls
CC2.1	User entities are responsible for the security and integrity of data housed under user entity control, particularly the data utilized by Iterative systems and services.
CC6.2	Determination of personnel who need specific functionality and the granting of such functionality is the responsibility of authorized personnel at the user entity. This includes allowing access to Iterative's application keys and API keys for access to the web service API.
CC6.3	Authorized users and their associated access are reviewed periodically.
CC6.6	User entities will ensure protective measures are in place for their data as it traverses from user entity to Iterative.
CC6.6	User entities should establish adequate physical security and environmental controls of all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity in order to provide authorized information to Iterative.
C1.1	User entities assign responsibility to personnel, and those personnel identify which data used by Iterative is to be considered "sensitive".

DC 7: Complementary Subservice Organization Controls

Although the subservice organization has been "**carved out**" for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization. Complementary Subservice Organization Controls (CSOCs) are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities. Management of Iterative receives and reviews the AWS SOC2 report annually. In addition, through its operational activities, Iterative management monitors the services performed by AWS to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with the service agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to AWS.

It is not feasible for the criteria related to the System to be achieved solely by Iterative. Therefore, each user entity's internal control must be evaluated in conjunction with Iterative's controls and related tests, and results described in Section 4 of this report, considering the related CSOCs expected to be implemented at the subservice organization as described below.

Criteria	Complementary Subservice Organization Controls
CC6.4	AWS is responsible for restricting data center access to authorized personnel.
CC6.4	AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC7.2 A1.2	AWS is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2 A1.2	AWS is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2 A1.2	AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

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

Physical Security - system is cloud hosted and managed. Company holds no critical physical infrastructure.

Availability - No HA SLAs are guaranteed as of date. intermittent service unavailabilities may occur.

DC 9: Disclosure of Significant Changes in Last 1 year

Changes to the services provided:

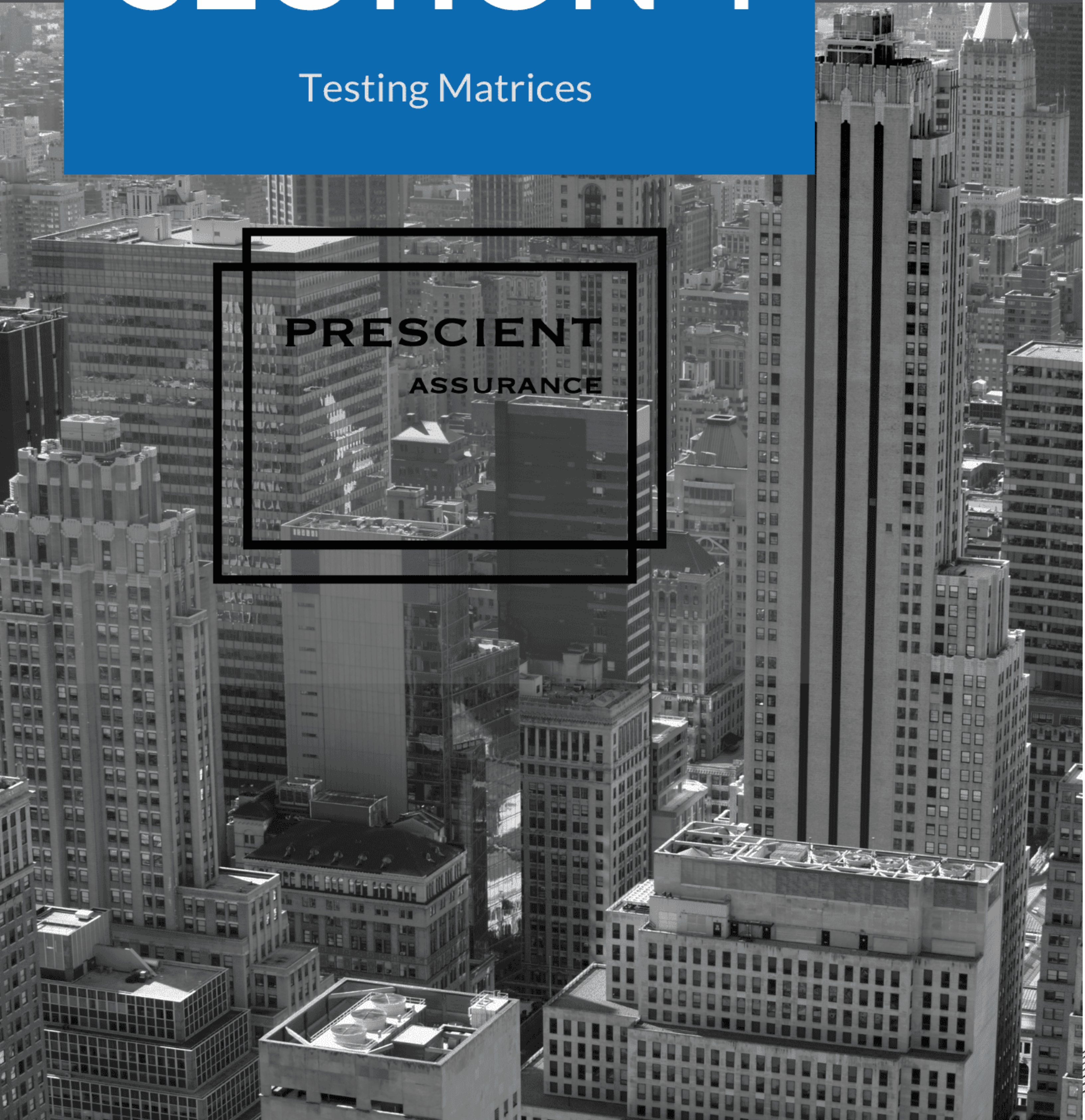
- Launched https://iterative.ai/model-registry
- Created Billing / Subscription plans (Team plan uses Stripe) - https://iterative.ai/pricing
- Some aspects of the system now have public access (public model registry) for leadgen and marketing purposes. No sensitive information was exposed there.
- Revamped self-hosting option for customers per demand - including publishing and supporting a helm-chart for self hosting.
- Monitoring - Started using mixpanel for analytics
- Introduced new features around experiment management and model registry

Significant changes to personnel / org structure:

- Hired 2 Backend Engineers
- Frontend Engineer moved to Studio from a different Team.
- Went through headcount reduction in Feb 2023 - >20% overall. .

SECTION 4

Testing Matrices



PRESCIENT ASSURANCE

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

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

Prescient Assurance LLC conducted the examination testing throughout the period April 17, 2023, to July 17, 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.		

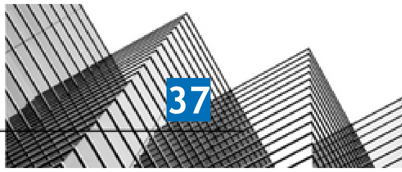
Reliability of Information Provided by the Service Organization

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
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	System tools monitors for uptime and availability based on predetermined criteria.	Observed that load balancers are utilized in AWS and Heroku, AWS EC2 instances are monitored in accordance with a set threshold, and AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch to determine that system tools are utilized to monitor for uptime and availability.	No exceptions noted.
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.	Inspected the Information Security Policy to determine that the company is required to collect and monitor audit logs and alerts, and is required to use logging solutions or SIEM tools to collect event information. Observed a list of logged events in Elastic to determine that logging and monitoring software is utilized by the company. Observed the Grafana dashboard showing various metrics being monitored to determine that the company uses Grafana to monitor its cloud infrastructure.	No exceptions noted.

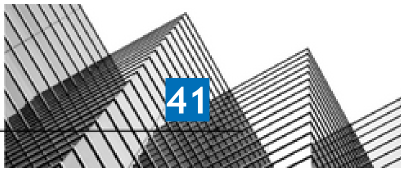


			Inspected an internal Slack channel showing an automated message from AlertManager notifying the company of an issue to determine that monitoring and alerting are enabled on the company's infrastructure. Observed that AWS RDS logs are ingested in CloudWatch, AWS EC2 security groups are configured for least functionality, AWS VPC flow logs are enabled, AWS Application load balancers have access logging enabled, CloudTrail is enabled for all regions within an account, log file integrity validation is enabled in CloudWatch, AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch, S3 buckets storing CloudTrail logs have server access logs enabled, GuardDuty is enabled for all accounts, AWS OpenSearch Service logs are published to CloudWatch, AWS CloudTrail is integrated with CloudWatch, AWS EKS logs are sent to CloudWatch, and most of the AWS S3 buckets have server access logs enabled.	
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	The system is configured for high availability to support continuous availability, when applicable.	Observed that AWS RDS instances are configured to scale across multiple availability zones, load balancers are utilized in Heroku and AWS, AWS EC2 auto-scaling groups (ASG) are configured to scale across multiple availability zones, autoscaling is configured for Heroku dynos, and availability zones are utilized in Heroku to promote high availability.	No exceptions noted.
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected the Network Security Policy to determine that the company is required to use monitoring solutions to detect network-based threats and generate alerts. Observed the Grafana dashboard showing various metrics being monitored to determine that the company uses Grafana to monitor its cloud infrastructure. Inspected an internal Slack channel showing an automated message from AlertManager notifying the company of an issue in AWS to determine that monitoring and alerting are enabled on the company's infrastructure. Observed the company's WAF rules in Cloudflare to determine that WAFs are utilized by the company. Observed that GuardDuty is enabled for all	No exceptions noted.

			accounts and AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch to determine that security tools have been implemented by the company to provide monitoring of network traffic to the production environment.	
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	Business Continuity and Disaster Recovery Policy governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Inspected the Business Continuity and Disaster Recovery Policy to determine that the recovery stage begins with the restoration of the company's services in an available commercial cloud provider's region, for Engineering.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	Full backups are performed and retained in accordance with the Business Continuity and Disaster Recovery Policy.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the company requires backups to be performed and retained for at least 30 days. Observed that AWS RDS instances are configured to enable automated backup, AWS RDS instances are configured to enable backups to be restored to a recent restore point, datastore backups for Heroku databases are retained, and Heroku Logplex automatically retains logs to determine that full backups are performed and retained by the company. Inspected a BCP test exercise that included a test scenario and showed an instance restored to a dedicated subdomain to determine that backup restoration testing is performed at the company.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment and Treatment Policy to determine that the company is required to perform risk assessments at least annually. Inspected the risk assessment questionnaire, which includes risk categories and responses to specific questions related to diverse risks to determine that the company performs a formal risk assessment annually.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery	The system is configured for high availability to support continuous availability, when applicable.	Observed that AWS RDS instances are configured to scale across multiple availability zones, load balancers are utilized in Heroku and AWS, AWS EC2 auto-scaling groups (ASG) are configured to scale across multiple availability zones, autoscaling is configured for Heroku dynos, and availability zones are utilized in Heroku to promote high availability.	No exceptions noted.

	infrastructure to meet its objectives.			
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company has established an incident response plan that provides guidelines for detecting, reporting, responding, and tracking incidents to resolution.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.	Inspected the Information Security Policy to determine that the company is required to collect and monitor audit logs and alerts, and is required to use logging solutions or SIEM tools to collect event information. Observed a list of logged events in Elastic to determine that logging and monitoring software is utilized by the company. Observed the Grafana dashboard showing various metrics being monitored to determine that the company uses Grafana to monitor its cloud infrastructure. Inspected an internal Slack channel showing an automated message from AlertManager notifying the company of an issue to determine that monitoring and alerting are enabled on the company's infrastructure. Observed that AWS RDS logs are ingested in CloudWatch, AWS EC2 security groups are configured for least functionality, AWS VPC flow logs are enabled, AWS Application load balancers have access logging enabled, CloudTrail is enabled for all regions within an account, log file integrity validation is enabled in CloudWatch, AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch, S3 buckets storing CloudTrail logs have server access logs enabled, GuardDuty is enabled for all accounts, AWS OpenSearch Service logs are published to CloudWatch, AWS CloudTrail is integrated with CloudWatch, AWS EKS logs are sent to CloudWatch, and most of the AWS S3 buckets have server access logs enabled.	No exceptions noted.

A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	System tools monitors for uptime and availability based on predetermined criteria.	Observed that load balancers are utilized in AWS and Heroku, AWS EC2 instances are monitored in accordance with a set threshold, and AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch to determine that system tools are utilized to monitor for uptime and availability.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Business Continuity and Disaster Recovery Policy governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Inspected the Business Continuity and Disaster Recovery Policy to determine that the recovery stage begins with the restoration of the company's services in an available commercial cloud provider's region, for Engineering.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The Business Continuity and Disaster Recovery Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Business Continuity and Disaster Recovery Plan based on the test results.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the company is required to test the plan through tabletop exercises and walkthroughs. Inspected the tabletop exercises held on May 25, 2023, which included test scenarios, the disaster, response, and recovery phases, and the key learnings to determine that the company tests the Business Continuity and Disaster Recovery Plan annually via tabletop exercises.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Backed-up data is restored to a non-production environment at least annually to validate the integrity of backups.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the company requires backups to be periodically tested to ensure that backups are sufficient and reliable. Inspected a BCP test exercise that included a test scenario and showed an instance restored to a dedicated subdomain to determine that backup restoration testing is performed at the company to validate the integrity of backups.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Personnel are assigned unique IDs to access sensitive systems, networks, and information.	Inspected the Access Control and Termination Policy to determine that the company is required to provide users with unique credentials to access systems and applications. Observed the personnel list maintained on Secureframe to determine that all personnel have been assigned unique emails.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	Inspected the Access Control and Termination Policy to determine that the company is required to provide users unique access keys and restrict access to systems and applications based on the principle of least privilege.	No exceptions noted.



			Inspected the AWS resource data to determine that AWS EC2 instances require associated keys for password-less secure shell (SSH) login and monitoring of AWS canary-token access key activity is enabled.	
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Upon customer request, Company requires that data that is no longer needed from databases and other file stores is removed in accordance with agreed-upon customer.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement. Observed open search dashboard to determine that upon customer request, Company requires that data that is no longer needed from databases and other file stores is removed in accordance with agreed-upon customer.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Service data transmitted over the internet is encrypted-in-transit.	Inspected the Encryption and Key Management Policy to determine that the company is required to use strong security protocols such as TLS 1.3 or at a minimum, TLS 1.1 protocol to encrypt the data transmitted over the Internet. Inspected the security certificate of the company's website which is valid until September 7, 2023, to determine that the company encrypts data in transit. Inspected the AWS resource data to determine that AWS ElasticSearch domains are configured to use node-to-node encryption and enforce HTTPS connections.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Company endpoints are managed and configured with anti-virus, and hard drive encryption.	Inspected the Configuration and Asset Management Policy to determine that the company requires user endpoint storage to be encrypted, malware protection to be enabled, and passwords to be of at least 8 characters and be complex. Observed that all relevant endpoints managed with Kolide have anti-malware software installed and hard drive encryption enabled to determine that company endpoints are configured with anti-virus and hard drive encryption. Inspected the Security and Privacy settings of a macOS device showing that FileVault is	No exceptions noted.

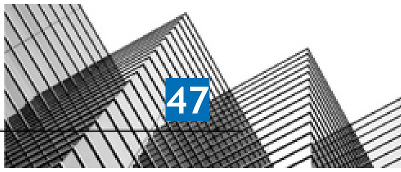
			enabled to determine that company endpoints have hard drive encryption enabled.	
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Access to, erasure of, or destruction of customer data is restricted to personnel that need access based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to provide users unique access keys and restrict access to systems and applications based on the principle of least privilege. Inspected the AWS resource data to determine that AWS IAM policies are not connected directly to user accounts, AWS EC2 instances require associated keys for password-less secure shell (SSH) login, and the AWS root account has limited usage. Inspected a list of device data to determine that the company settings are configured to enforce hard drive encryption for each connected device.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Service data is encrypted-at-rest.	Inspected the Encryption and Key Management Policy to determine that the company is required to use the NIST protocols for data encryption at rest. Inspected the AWS resource data to determine that AWS RDS instances, EFS volumes, RDS snapshots, SSM parameters, EBS snapshots, Athena workgroups, and ElasticSearch domains are configured to be encrypted at rest.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected the Vendor Management Policy to determine that the company is required to conduct a risk assessment and due diligence for new vendors before engaging with them and a designee is responsible for annual re-reviews of high-risk vendors. Inspected a vendor directory, which shows a list of vendors with their associated risk levels and review dates to determine that vendors are assessed and reviewed annually in accordance with their risk levels. Inspected a master services agreement signed between the company and Lost Rabbit Labs which included confidentiality clauses to determine that the company signs formal agreements with vendors.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	A Data Retention and Disposal Policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a	No exceptions noted.

			customer or in accordance with the agreement.	
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Business Continuity and Disaster Recovery Policy governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Inspected the Business Continuity and Disaster Recovery Policy to determine that the recovery stage begins with the restoration of the company's services in an available commercial cloud provider's region, for Engineering.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Procedures are in place to retain customer data based on agreed-upon customer requirements or in line with information security policies.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Terms of Service or the equivalent are published or shared to external users.	Inspected the Terms and Conditions and MSA template to determine that the user agreement and service commitments are communicated to internal personnel and external users.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	Inspected the Encryption and Key Management Policy to determine that the company has defined the guidelines and requirements for data encryption and cryptographic key management.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to grant users administrative access to the production infrastructure based on the principle of least privilege. Observed the list of AWS IAM users and user access tracking to determine that the no-user access list and tracking is tested during the audit period. Inspected the AWS resource data to determine that AWS S3 buckets permission is granted via ACL and the root account is not used for day-to-day account management.	No exceptions noted.
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to grant users administrative access to the production infrastructure based on the principle of least privilege. Observed the list of AWS IAM users and user access tracking to determine that the no-user	No exceptions noted.

			access list and tracking is tested during the audit period. Inspected the AWS resource data to determine that AWS S3 buckets permission is granted via ACL and the root account is not used for day-to-day account management.	
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	A Data Classification Policy details the security and handling protocols for sensitive data.	Inspected the Data Classification Policy to determine that the company has identified the types of confidential, internal, public, and restricted data that is collected and the processes for labeling, handling, storing, and deleting such information.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Procedures are in place to retain customer data based on agreed-upon customer requirements or in line with information security policies.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	A Data Classification Policy details the security and handling protocols for sensitive data.	Inspected the Data Classification Policy to determine that the company has identified the types of confidential, internal, public, and restricted data that is collected and the processes for labeling, handling, storing, and deleting such information.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Upon customer request, Company requires that data that is no longer needed from databases and other file stores is removed in accordance with agreed-upon customer.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement. Observed open search dashboard to determine that upon customer request, Company requires that data that is no longer needed from databases and other file stores is removed in accordance with agreed-upon customer.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	A Data Retention and Disposal Policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement.	No exceptions noted.

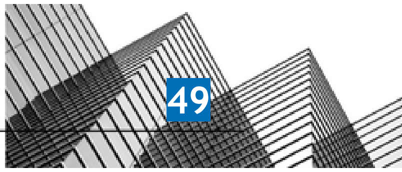
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Inspected the Information Security Policy, Code of Conduct, and Acceptable Use Policy to determine that the disciplinary actions including termination of employment against violation of security policies and procedures have been described.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inspected minutes of a meeting of the board to determine that the board of directors meets at least annually to review business goals, company initiatives and other internal/external matters. Inspected agenda of a quarterly security meeting to determine that the information security team meets quarterly to discuss security risks and/or other matters as necessary.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	A Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	Inspected the Code of Conduct to determine that the company has defined ethical expectations against business standards and the consequences of violating these standards.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from the company's operations. An information security team has also been established to govern cybersecurity.	Inspected the bylaws of the company to determine that Board of Directors bylaws are established to provide corporate oversight, strategic direction, and review of management. Inspected the data to determine that the company has established a 4-member information security team including an information security manager.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Internal personnel are evaluated via a formal performance review at least annually.	Inspected the Performance Review Policy to determine that all employees are required to undergo a performance evaluation process annually. Inspected the performance evaluation of an employee to determine that internal personnel are evaluated via a formal performance review at least annually.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote	Inspected the Internal Control Policy to determine that the company has defined the guidelines to maintain the internal control system and to protect its assets, stating that it	No exceptions noted.

		operational efficiency, and encourage adherence to prescribed managerial policies.	uses Secureframe to manage and maintain its internal controls.	
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from the company's operations. An information security team has also been established to govern cybersecurity.	Inspected the bylaws of the company to determine that Board of Directors bylaws are established to provide corporate oversight, strategic direction, and review of management. Inspected the data to determine that the company has established a 4-member information security team including an information security manager.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inspected minutes of a meeting of the board to determine that the board of directors meets at least annually to review business goals, company initiatives and other internal/external matters. Inspected agenda of a quarterly security meeting to determine that the information security team meets quarterly to discuss security risks and/or other matters as necessary.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Internal personnel are evaluated via a formal performance review at least annually.	Inspected the Performance Review Policy to determine that all employees are required to undergo a performance evaluation process annually. Inspected the performance evaluation of an employee to determine that internal personnel are evaluated via a formal performance review at least annually.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart to internal personnel.	Observed an organizational chart to determine that management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities	An Acceptable Use Policy defines standards for appropriate and secure use of company hardware and electronic systems	Inspected the Acceptable Use Policy to determine that the company has defined the standards for appropriate and secure use of hardware and electronic systems including	No exceptions noted.

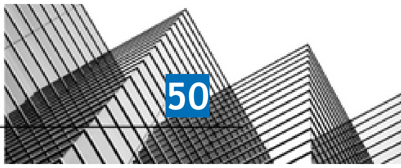


	and responsibilities in the pursuit of objectives.	including storage media, communication tools and internet access.	storage media, communication tools, and internet access.	
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected the Vendor Management Policy to determine that the company is required to conduct annual reviews of vendors, which may include the gathering of applicable compliance audits such as SOC 1, SOC 2, PCI HITRUST, ISO 27001 and others. Inspected the Vetty Customer Terms of Services document to determine that vendors' compliance reports have been collected by 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.	A Data Classification Policy details the security and handling protocols for sensitive data.	Inspected the Data Classification Policy to determine that the company has identified the types of confidential, internal, public, and restricted data that is collected and the processes for labeling, handling, storing, and deleting such information.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from the company's operations. An information security team has also been established to govern cybersecurity.	Inspected the bylaws of the company to determine that Board of Directors bylaws are established to provide corporate oversight, strategic direction, and review of management. Inspected the data to determine that the company has established a 4-member information security team including an information security manager.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	An Information Security Policy establishes the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	Inspected the Information Security Policy to determine that the company has established requirements to maintain a secure information security posture.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results	Inspected minutes of a meeting of the board to determine that the board of directors meets at least annually to review business goals, company initiatives and other internal/external matters. Inspected agenda of a quarterly security meeting to determine that the information security team meets quarterly to discuss security risks and/or other matters as necessary.	No exceptions noted.

		and/or other matters as necessary.		
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Information security roles and responsibilities are outlined for personnel responsible for the security, availability, and confidentiality of the system.	Inspected the Internal Control Policy, Performance Review Policy, and Security Incident Response Plan, to determine that the information security responsibilities of the senior management, managers, and the security response team have been documented. Inspected a sample of job descriptions for various positions to determine that the company outlines the roles and responsibilities in relevant job descriptions.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected the Vendor Management Policy to determine that the company is required to conduct a risk assessment and due diligence for new vendors before engaging with them and a designee is responsible for annual re-reviews of high-risk vendors. Inspected a vendor directory, which shows a list of vendors with their associated risk levels and review dates to determine that vendors are assessed and reviewed annually in accordance with their risk levels. Inspected a master services agreement signed between the company and Lost Rabbit Labs which included confidentiality clauses to determine that the company signs formal agreements with vendors.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected the Vendor Management Policy to determine that the company is required to conduct a risk assessment and due diligence for new vendors before engaging with them and a designee is responsible for annual re-reviews of high-risk vendors. Inspected a vendor directory, which shows a list of vendors with their associated risk levels and review dates to determine that vendors are assessed and reviewed annually in accordance with their risk levels. Inspected a master services agreement signed between the company and Lost Rabbit Labs which included confidentiality clauses to determine that the company signs formal agreements with vendors.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain	A Data Classification Policy details the security and handling protocols for sensitive data.	Inspected the Data Classification Policy to determine that the company has identified the types of confidential, internal, public, and restricted data that is collected and the	No exceptions noted.

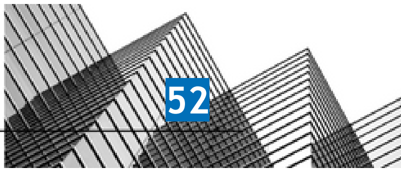


	competent individuals in alignment with objectives.		processes for labeling, handling, storing, and deleting such information.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company has established an incident response plan that provides guidelines for detecting, reporting, responding, and tracking incidents to resolution.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	Inspected the Code of Conduct to determine that the company has defined ethical expectations against business standards and the consequences of violating these standards.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Internal personnel are evaluated via a formal performance review at least annually.	Inspected the Performance Review Policy to determine that all employees are required to undergo a performance evaluation process annually. Inspected the performance evaluation of an employee to determine that internal personnel are evaluated via a formal performance review at least annually.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy to determine that the company has defined the guidelines to maintain the internal control system and to protect its assets, stating that it uses Secureframe to manage and maintain its internal controls.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from the company's operations. An information security team has also been established to govern cybersecurity.	Inspected the bylaws of the company to determine that Board of Directors bylaws are established to provide corporate oversight, strategic direction, and review of management. Inspected the data to determine that the company has established a 4-member information security team including an information security manager.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	An Acceptable Use Policy defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools and internet access.	Inspected the Acceptable Use Policy to determine that the company has defined the standards for appropriate and secure use of hardware and electronic systems including storage media, communication tools, and internet access.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain	Information security roles and responsibilities are outlined for personnel	Inspected the Internal Control Policy, Performance Review Policy, and Security Incident Response Plan, to determine that the	No exceptions noted.



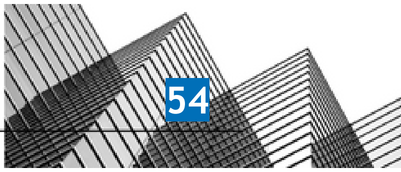
	competent individuals in alignment with objectives.	responsible for the security, availability, and confidentiality of the system.	information security responsibilities of the senior management, managers, and the security response team have been documented. Inspected a sample of job descriptions for various positions to determine that the company outlines the roles and responsibilities in relevant job descriptions.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	An Information Security Policy establishes the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	Inspected the Information Security Policy to determine that the company has established requirements to maintain a secure information security posture.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected the Vendor Management Policy to determine that the company is required to conduct annual reviews of vendors, which may include the gathering of applicable compliance audits such as SOC 1, SOC 2, PCI HITRUST, ISO 27001 and others. Inspected the Vetty Customer Terms of Services document to determine that vendors' compliance reports have been collected by the company.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Vulnerability Management and Patch Management Policy outlines the processes to efficiently respond to identified vulnerabilities.	Inspected the Vulnerability and Patch Management Policy to determine that the company has established the processes for vulnerability management including scan requirements and remediation strategies.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Data Retention and Disposal Policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Privacy Policy to both external users and internal personnel. This policy details the company's privacy commitments.	Inspected the privacy policy document to determine that the company has communicated its privacy and security commitments to external users and internal personnel.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats,	Inspected the Risk Assessment and Treatment Policy to determine that a policy is in place which governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with	No exceptions noted.

		vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy. Observed the policy acceptance data for the company's Risk Assessment and Treatment Policy to determine that all of the in-scope personnel have accepted the policy and that the policy has been approved within the last year.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security.	Inspected the Information Security Policy to determine that internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security. Observed the training completion records for in-scope personnel to determine that all of the personnel have completed annual training programs for information security to help them understand their obligations and responsibilities related to security.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill their responsibilities. New hires sign confidentiality agreements or equivalents upon hire.	Observed a sample of job candidates' resumes to determine that hiring managers screen candidates on the basis of their qualifications, experience, and competency to fulfill the responsibilities of the position. Observed the company's confidentiality agreement to determine that the company requires new hires to sign confidentiality agreements upon hire. Observed the company's careers page to determine that the company's expectations for candidates applying to open positions are formally expressed.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected the Secure Development Policy to determine that a policy is in place which defines the requirements for secure software and system development and maintenance. Observed the policy acceptance data for the company's Secure Development Policy to determine that all of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Vendor Risk Management Policy defines a framework for the onboarding and management of the	Inspected the Vendor Management Policy to determine that a policy is in place and defines a framework for the onboarding and management of the vendor relationship lifecycle.	No exceptions noted.

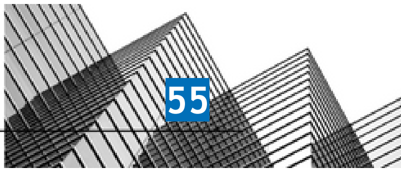


		vendor relationship lifecycle.	Observed the policy acceptance data for the company's Vendor Management Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected the Change Management Policy to determine that a policy is in place which governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes. Observed the policy acceptance data for the company's Change Management Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Inspected the Performance Review Policy to determine that a policy is in place which provides personnel context and transparency into their performance and career development processes. Observed the policy acceptance data for the company's Performance Review Policy to determine that all of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Background checks or their equivalent are performed before or promptly after a new hires start date, as permitted by local laws.	Inspected the Information Security Policy to determine that all personnel are required to complete a background check. Observed an employee's background check report to determine that the company uses a third-party service to conduct background checks. Observed the personnel data to determine that background checks have been performed for all of the personnel.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Management is responsible for the design, implementation, and management of the organization's security policies and procedures. The policies and procedures are reviewed by management at least annually.	Inspected the Information Security Policy to determine that internal personnel review and accept applicable information security policies at least annually. Observed the company's Information Security Policy, Access Control and Termination Policy, Change Management Policy, Risk Assessment and Treatment Policy, and Secure Development Policy, among others, to determine that they have been reviewed within the last year.	No exceptions noted.

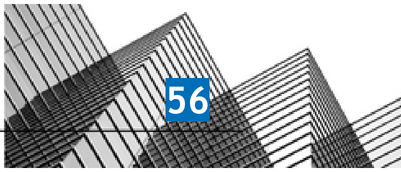
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control and Termination Policy to determine that a policy governs authentication and access to applicable systems, data, and networks. Observed the policy acceptance data for the company's Access Control and Termination Policy to determine that most of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Internal personnel review and accept applicable information security policies at least annually.	Inspected the Information Security Policy to determine that internal personnel review and accept applicable information security policies at least annually. Observed the policy acceptance data to determine that the company's policies have been accepted by all of the internal personnel within the last year.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy to determine that a Network Security Policy is in place which identifies the requirements for protecting information and systems within and across networks. Observed the policy acceptance data for the company's Network Security Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Business Continuity and Disaster Recovery Policy governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Inspected the Business Continuity and Disaster Recovery Policy to determine that the recovery stage begins with the restoration of the company's services in an available commercial cloud provider’s region, for Engineering.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that the company has defined the minimum device configuration settings, including encryption, passwords, malware protection, and security updates.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	Inspected the Encryption and Key Management Policy to determine that the company has defined the guidelines and requirements for data encryption and cryptographic key management.	No exceptions noted.



CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Inspected the Performance Review Policy to determine that a policy is in place which provides personnel context and transparency into their performance and career development processes. Observed the policy acceptance data for the company's Performance Review Policy to determine that all of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart to internal personnel.	Observed an organizational chart to determine that management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy to determine that the company manages and maintains its internal controls through the use of the Secureframe platform. Observed that the company uses Secureframe to continuously monitor its internal security controls and SOC 2 security controls have owners.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inspected minutes of a meeting of the board to determine that the board of directors meets at least annually to review business goals, company initiatives and other internal/external matters. Inspected agenda of a quarterly security meeting to determine that the information security team meets quarterly to discuss security risks and/or other matters as necessary.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from the company's operations. An information security team	Inspected the bylaws of the company to determine that Board of Directors bylaws are established to provide corporate oversight, strategic direction, and review of management. Inspected the data to determine that the company has established a 4-member	No exceptions noted.



		has also been established to govern cybersecurity.	information security team including an information security manager.	
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Inspected the Information Security Policy, Code of Conduct, and Acceptable Use Policy to determine that the disciplinary actions including termination of employment against violation of security policies and procedures have been described.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Internal personnel are evaluated via a formal performance review at least annually.	Inspected the Performance Review Policy to determine that all employees are required to undergo a performance evaluation process annually. Inspected the performance evaluation of an employee to determine that internal personnel are evaluated via a formal performance review at least annually.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill their responsibilities. New hires sign confidentiality agreements or equivalents upon hire.	Observed a sample of job candidates' resumes to determine that hiring managers screen candidates on the basis of their qualifications, experience, and competency to fulfill the responsibilities of the position. Observed the company's confidentiality agreement to determine that the company requires new hires to sign confidentiality agreements upon hire. Observed the company's careers page to determine that the company's expectations for candidates applying to open positions are formally expressed.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy to determine that the company has defined the guidelines to maintain the internal control system and to protect its assets, stating that it uses Secureframe to manage and maintain its internal controls.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment and Treatment Policy to determine that the company is required to perform risk assessments at least annually. Inspected the risk assessment questionnaire, which includes risk categories and responses to specific questions related to diverse risks to determine that the company performs a formal risk assessment annually.	No exceptions noted.



CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected the Vulnerability and Patch Management Policy to determine that the company performs vulnerability scans periodically. Inspected a list of common vulnerabilities to determine that vulnerability scans are performed on applicable internal infrastructure. Inspected a list of images scanned for vulnerabilities on Sysdig Secure platform to determine that external vulnerability scans are performed on internet-facing infrastructure. Inspected to determine that security vulnerabilities and threats are tracked to resolution, as per applicable SLAs.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy to determine that the company manages and maintains its internal controls through the use of the Secureframe platform. Observed that the company uses Secureframe to continuously monitor its internal security controls and SOC 2 security controls have owners.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy to determine that the company requires software changes to be tested in the staging environment before release to production. Inspected the testing data showing that code integration, dependency, and static application security testing is performed in GitHub to determine that software changes are tested prior to being deployed into production.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	A 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Inspected the Vulnerability and Patch Management Policy to determine that the company schedules third party security assessments and penetration tests at least annually. Observed performed penetration test to determine that a 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	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.	Information security roles and responsibilities are outlined for personnel responsible for the security, availability, and confidentiality of the system.	Inspected the Internal Control Policy, Performance Review Policy, and Security Incident Response Plan, to determine that the information security responsibilities of the senior management, managers, and the security response team have been documented. Inspected a sample of job descriptions for various positions to determine that the company outlines the roles and responsibilities in relevant job descriptions.	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.	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inspected the Security Incident Response Plan to determine that the company requires its security response team (SRT) to document, assess, and respond to security incidents according to the incident response process. Inspected details of a resolved security issue on GitHub dashboard to determine that identified incidents are documented, tracked, analyzed, and resolved.	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.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company has established an incident response plan that provides guidelines for detecting, reporting, responding, and tracking incidents to resolution.	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.	An Acceptable Use Policy defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools and internet access.	Inspected the Acceptable Use Policy to determine that the company has defined the standards for appropriate and secure use of hardware and electronic systems including storage media, communication tools, and internet access.	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.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected the Configuration and Asset Management Policy to determine that the company requires production systems handling confidential data to have documented baseline configurations. Inspected details of cryptographic keys used in different scopes to determine that baseline settings and/or vendor documentation are utilized for configuring cloud services or on-premise servers.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to	An Information Security Policy establishes the security requirements for maintaining the security, confidentiality, integrity, and availability of	Inspected the Information Security Policy to determine that the company has established requirements to maintain a secure information security posture.	No exceptions noted.

	support the functioning of internal control.	applications, systems, infrastructure, and data.		
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	A Data Classification Policy details the security and handling protocols for sensitive data.	Inspected the Data Classification Policy to determine that the company has identified the types of confidential, internal, public, and restricted data that is collected and the processes for labeling, handling, storing, and deleting such information.	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.	Management is responsible for the design, implementation, and management of the organization's security policies and procedures. The policies and procedures are reviewed by management at least annually.	Inspected the Information Security Policy to determine that internal personnel review and accept applicable information security policies at least annually. Observed the company's Information Security Policy, Access Control and Termination Policy, Change Management Policy, Risk Assessment and Treatment Policy, and Secure Development Policy, among others, to determine that they have been reviewed within the last year.	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.	Internal personnel review and accept applicable information security policies at least annually.	Inspected the Information Security Policy to determine that internal personnel review and accept applicable information security policies at least annually. Observed the policy acceptance data to determine that the company's policies have been accepted by all of the internal personnel within the last year.	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.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that the company has defined the minimum device configuration settings, including encryption, passwords, malware protection, and security updates.	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.	Terms of Service or the equivalent are published or shared to external users.	Inspected the Terms and Conditions and MSA template to determine that the user agreement and service commitments are communicated to internal personnel and external users.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	A Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	Inspected the Code of Conduct to determine that the company has defined ethical expectations against business standards and the consequences of violating these standards.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and	Development, staging, and production environments are segregated.	Inspected the Information Security Policy to determine that the company is required to maintain controls for the segregation of	No exceptions noted.

	responsibilities for internal control, necessary to support the functioning of internal control.		development and production environments. Inspected a list of separate folders for development and production to determine that development, staging, and production environments are segregated.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from the company's operations. An information security team has also been established to govern cybersecurity.	Inspected the bylaws of the company to determine that Board of Directors bylaws are established to provide corporate oversight, strategic direction, and review of management. Inspected the data to determine that the company has established a 4-member information security team including an information security manager.	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.	Internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security.	Inspected the Information Security Policy to determine that internal personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security. Observed the training completion records for in-scope personnel to determine that all of the personnel have completed annual training programs for information security to help them understand their obligations and responsibilities related to security.	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.	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy to determine that a Network Security Policy is in place which identifies the requirements for protecting information and systems within and across networks. Observed the policy acceptance data for the company's Network Security Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	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.	A Privacy Policy to both external users and internal personnel. This policy details the company's privacy commitments.	Inspected the privacy policy document to determine that the company has communicated its privacy and security commitments to external users and internal personnel.	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.	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence	Inspected the Internal Control Policy to determine that the company has defined the guidelines to maintain the internal control system and to protect its assets, stating that it uses Secureframe to manage and maintain its internal controls.	No exceptions noted.

		to prescribed managerial policies.		
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Security commitments and expectations are communicated to both internal personnel and external users via the company's website.	Inspected the Security and Privacy page on the company's website to determine that security commitments and expectations are communicated to both internal personnel and external users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy to determine that a Network Security Policy is in place which identifies the requirements for protecting information and systems within and across networks. Observed the policy acceptance data for the company's Network Security Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Procedures are in place to retain customer data based on agreed-upon customer requirements or in line with information security policies.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inspected the Security Incident Response Plan to determine that the company requires its security response team (SRT) to document, assess, and respond to security incidents according to the incident response process. Inspected details of a resolved security issue on GitHub dashboard to determine that identified incidents are documented, tracked, analyzed, and resolved.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Terms of Service or the equivalent are published or shared to external users.	Inspected the Terms and Conditions and MSA template to determine that the user agreement and service commitments are communicated to internal personnel and external users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected the Configuration and Asset Management Policy to determine that the company requires production systems handling confidential data to have documented baseline configurations. Inspected details of cryptographic keys used in different scopes to determine that baseline settings and/or vendor documentation are	No exceptions noted.

			utilized for configuring cloud services or on-premise servers.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	A Privacy Policy to both external users and internal personnel. This policy details the company's privacy commitments.	Inspected the privacy policy document to determine that the company has communicated its privacy and security commitments to external users and internal personnel.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Security commitments and expectations are communicated to both internal personnel and external users via the company's website.	Inspected the Security and Privacy page on the company's website to determine that security commitments and expectations are communicated to both internal personnel and external users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Development, staging, and production environments are segregated.	Inspected the Information Security Policy to determine that the company is required to maintain controls for the segregation of development and production environments. Inspected a list of separate folders for development and production to determine that development, staging, and production environments are segregated.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that the company has defined the minimum device configuration settings, including encryption, passwords, malware protection, and security updates.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Production data is not used in the development and testing environments, unless required for debugging customer issues.	Inspected the Secure Development Policy to determine that confidential and restricted data, as well as data that can be related to individual persons, should not be used as test data, and exceptions may be approved only by Oded Messer, in which case Oded Messer should define how such test data are protected. Observed AWS databases to determine that production data is not used in the development and testing environments, unless required for debugging customer issues.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	A confidential reporting channel is made available to internal personnel and external parties to report security and other identified concerns.	Inspected the Security Incident Response Plan to determine that an email address (security@iterative.ai) has been provided to internal personnel to report issues.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor.	Inspected the Vendor Management Policy to determine that the company is required to conduct a risk assessment and due diligence for new vendors before engaging with them and a designee is responsible for annual re-reviews of high-risk vendors.	No exceptions noted.

		Reassessment occurs at least annually.	Inspected a vendor directory, which shows a list of vendors with their associated risk levels and review dates to determine that vendors are assessed and reviewed annually in accordance with their risk levels. Inspected a master services agreement signed between the company and Lost Rabbit Labs which included confidentiality clauses to determine that the company signs formal agreements with vendors.	
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment and Treatment Policy to determine that the company is required to perform risk assessments at least annually. Inspected the risk assessment questionnaire, which includes risk categories and responses to specific questions related to diverse risks to determine that the company performs a formal risk assessment annually.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inspected minutes of a meeting of the board to determine that the board of directors meets at least annually to review business goals, company initiatives and other internal/external matters. Inspected agenda of a quarterly security meeting to determine that the information security team meets quarterly to discuss security risks and/or other matters as necessary.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Inspected the Risk Assessment and Treatment Policy to determine that a policy is in place which governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy. Observed the policy acceptance data for the company's Risk Assessment and Treatment Policy to determine that all of the in-scope personnel have accepted the policy and that	No exceptions noted.

			the policy has been approved within the last year.	
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.	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected the Vendor Management Policy to determine that the company is required to conduct a risk assessment and due diligence for new vendors before engaging with them and a designee is responsible for annual re-reviews of high-risk vendors. Inspected a vendor directory, which shows a list of vendors with their associated risk levels and review dates to determine that vendors are assessed and reviewed annually in accordance with their risk levels. Inspected a master services agreement signed between the company and Lost Rabbit Labs which included confidentiality clauses to determine that the company signs formal agreements with vendors.	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.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inspected minutes of a meeting of the board to determine that the board of directors meets at least annually to review business goals, company initiatives and other internal/external matters. Inspected agenda of a quarterly security meeting to determine that the information security team meets quarterly to discuss security risks and/or other matters as necessary.	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.	A list of system assets, components, and respective owners are maintained and reviewed at least annually.	Inspected the Configuration and Asset Management Policy to determine that the company is required to maintain an inventory of servers, desktops, laptops, and other devices used to store, create, modify, delete, or transmit confidential information. Inspected lists of user endpoints, AWS resources, and GitHub and Bitbucket repositories along with assigned owners to determine that the company maintains an inventory of system assets, components, and respective owners.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as	A Vendor Risk Management Policy defines a framework for the onboarding and	Inspected the Vendor Management Policy to determine that a policy is in place and defines a framework for the onboarding and management of the vendor relationship	No exceptions noted.

	a basis for determining how the risks should be managed.	management of the vendor relationship lifecycle.	lifecycle. Observed the policy acceptance data for the company's Vendor Management Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	
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.	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment and Treatment Policy to determine that the company is required to perform risk assessments at least annually. Inspected the risk assessment questionnaire, which includes risk categories and responses to specific questions related to diverse risks to determine that the company performs a formal risk assessment annually.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	A risk register is maintained, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	Inspected the Risk Assessment and Treatment Policy to determine that the company is required to document identified external and internal vulnerabilities and related threats along with risk responses as part of the company's risk assessment. Inspected the risk register which includes risk source, affected assets, vulnerabilities, impact, likelihood, treatment decisions, and residual risk to determine that a risk register is maintained.	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.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Inspected the Risk Assessment and Treatment Policy to determine that a policy is in place which governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy. Observed the policy acceptance data for the company's Risk Assessment and Treatment Policy to determine that all of the in-scope personnel have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors,	Inspected the Risk Assessment and Treatment Policy to determine that a policy is in place which governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	No exceptions noted.

		suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Observed the policy acceptance data for the company's Risk Assessment and Treatment Policy to determine that all of the in-scope personnel have accepted the policy and that the policy has been approved within the last year.	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment and Treatment Policy to determine that the company is required to perform risk assessments at least annually. Inspected the risk assessment questionnaire, which includes risk categories and responses to specific questions related to diverse risks to determine that the company performs a formal risk assessment annually.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected the Vendor Management Policy to determine that the company is required to conduct a risk assessment and due diligence for new vendors before engaging with them and a designee is responsible for annual re-reviews of high-risk vendors. Inspected a vendor directory, which shows a list of vendors with their associated risk levels and review dates to determine that vendors are assessed and reviewed annually in accordance with their risk levels. Inspected a master services agreement signed between the company and Lost Rabbit Labs which included confidentiality clauses to determine that the company signs formal agreements with vendors.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Inspected the Vendor Management Policy to determine that a policy is in place and defines a framework for the onboarding and management of the vendor relationship lifecycle. Observed the policy acceptance data for the company's Vendor Management Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence	Inspected the Internal Control Policy to determine that the company has defined the guidelines to maintain the internal control system and to protect its assets, stating that it uses Secureframe to manage and maintain its internal controls.	No exceptions noted.

		to prescribed managerial policies.		
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment and Treatment Policy to determine that the company is required to perform risk assessments at least annually. Inspected the risk assessment questionnaire, which includes risk categories and responses to specific questions related to diverse risks to determine that the company performs a formal risk assessment annually.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Procedures are in place to retain customer data based on agreed-upon customer requirements or in line with information security policies.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Inspected the Risk Assessment and Treatment Policy to determine that a policy is in place which governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy. Observed the policy acceptance data for the company's Risk Assessment and Treatment Policy to determine that all of the in-scope personnel have accepted the policy and that the policy has been approved within the last year.	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.	A 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Inspected the Vulnerability and Patch Management Policy to determine that the company schedules third party security assessments and penetration tests at least annually. Observed performed penetration test to determine that a 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy to determine that the company requires software changes to be tested in the staging environment before release to production.	No exceptions noted.

	internal control are present and functioning.		Inspected the testing data showing that code integration, dependency, and static application security testing is performed in GitHub to determine that software changes are tested prior to being deployed into production.	
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.	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected the Vulnerability and Patch Management Policy to determine that the company performs vulnerability scans periodically. Inspected a list of common vulnerabilities to determine that vulnerability scans are performed on applicable internal infrastructure. Inspected a list of images scanned for vulnerabilities on Sysdig Secure platform to determine that external vulnerability scans are performed on internet-facing infrastructure. Inspected to determine that security vulnerabilities and threats are tracked to resolution, as per applicable SLAs.	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.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy to determine that the company manages and maintains its internal controls through the use of the Secureframe platform. Observed that the company uses Secureframe to continuously monitor its internal security controls and SOC 2 security controls have owners.	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.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inspected minutes of a meeting of the board to determine that the board of directors meets at least annually to review business goals, company initiatives and other internal/external matters. Inspected agenda of a quarterly security meeting to determine that the information security team meets quarterly to discuss security risks and/or other matters as necessary.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a	Vulnerability scanning is performed on production infrastructure systems,	Inspected the Vulnerability and Patch Management Policy to determine that the company performs vulnerability scans	No exceptions noted.

	timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	and identified deficiencies are remediated on a timely basis.	periodically. Inspected a list of common vulnerabilities to determine that vulnerability scans are performed on applicable internal infrastructure. Inspected a list of images scanned for vulnerabilities on Sysdig Secure platform to determine that external vulnerability scans are performed on internet-facing infrastructure. Inspected to determine that security vulnerabilities and threats are tracked to resolution, as per applicable SLAs.	
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.	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy to determine that the company requires software changes to be tested in the staging environment before release to production. Inspected the testing data showing that code integration, dependency, and static application security testing is performed in GitHub to determine that software changes are tested prior to being deployed into production.	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.	A 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Inspected the Vulnerability and Patch Management Policy to determine that the company schedules third party security assessments and penetration tests at least annually. Observed performed penetration test to determine that a 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	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.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy to determine that the company manages and maintains its internal controls through the use of the Secureframe platform. Observed that the company uses Secureframe to continuously monitor its internal security controls and SOC 2 security controls have owners.	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.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inspected minutes of a meeting of the board to determine that the board of directors meets at least annually to review business goals, company initiatives and other internal/external matters. Inspected agenda of a quarterly security meeting to determine that the information security team meets quarterly to discuss security risks and/or other matters as necessary.	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.	A risk register is maintained, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	Inspected the Risk Assessment and Treatment Policy to determine that the company is required to document identified external and internal vulnerabilities and related threats along with risk responses as part of the company's risk assessment. Inspected the risk register which includes risk source, affected assets, vulnerabilities, impact, likelihood, treatment decisions, and residual risk to determine that a risk register is maintained.	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.	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment and Treatment Policy to determine that the company is required to perform risk assessments at least annually. Inspected the risk assessment questionnaire, which includes risk categories and responses to specific questions related to diverse risks to determine that the company performs a formal risk assessment 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.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy to determine that the company manages and maintains its internal controls through the use of the Secureframe platform. Observed that the company uses Secureframe to continuously monitor its internal security controls and SOC 2 security controls have owners.	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.	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency,	Inspected the Internal Control Policy to determine that the company has defined the guidelines to maintain the internal control system and to protect its assets, stating that it uses Secureframe to manage and maintain its internal controls.	No exceptions noted.

		and encourage adherence to prescribed managerial policies.		
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inspected minutes of a meeting of the board to determine that the board of directors meets at least annually to review business goals, company initiatives and other internal/external matters. Inspected agenda of a quarterly security meeting to determine that the information security team meets quarterly to discuss security risks and/or other matters as necessary.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy to determine that the company manages and maintains its internal controls through the use of the Secureframe platform. Observed that the company uses Secureframe to continuously monitor its internal security controls and SOC 2 security controls have owners.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	A list of system assets, components, and respective owners are maintained and reviewed at least annually.	Inspected the Configuration and Asset Management Policy to determine that the company is required to maintain an inventory of servers, desktops, laptops, and other devices used to store, create, modify, delete, or transmit confidential information. Inspected lists of user endpoints, AWS resources, and GitHub and Bitbucket repositories along with assigned owners to determine that the company maintains an inventory of system assets, components, and respective owners.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	An Information Security Policy establishes the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	Inspected the Information Security Policy to determine that the company has established requirements to maintain a secure information security posture.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology	An Internal Control Policy identifies how a system of controls should be maintained to safeguard	Inspected the Internal Control Policy to determine that the company has defined the guidelines to maintain the internal control system and to protect its assets, stating that it	No exceptions noted.

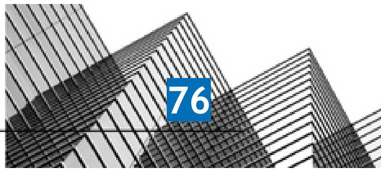
	to support the achievement of objectives.	assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	uses Secureframe to manage and maintain its internal controls.	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Information security roles and responsibilities are outlined for personnel responsible for the security, availability, and confidentiality of the system.	Inspected the Internal Control Policy, Performance Review Policy, and Security Incident Response Plan, to determine that the information security responsibilities of the senior management, managers, and the security response team have been documented. Inspected a sample of job descriptions for various positions to determine that the company outlines the roles and responsibilities in relevant job descriptions.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected the Secure Development Policy to determine that a policy is in place which defines the requirements for secure software and system development and maintenance. Observed the policy acceptance data for the company's Secure Development Policy to determine that all of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	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.	A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Inspected the Vendor Management Policy to determine that a policy is in place and defines a framework for the onboarding and management of the vendor relationship lifecycle. Observed the policy acceptance data for the company's Vendor Management Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	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.	Management is responsible for the design, implementation, and management of the organization's security policies and procedures. The policies and procedures are reviewed by management at least annually.	Inspected the Information Security Policy to determine that internal personnel review and accept applicable information security policies at least annually. Observed the company's Information Security Policy, Access Control and Termination Policy, Change Management Policy, Risk Assessment and Treatment Policy, and Secure Development Policy, among others, to determine that they have been reviewed within the last year.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in	A Vulnerability Management and Patch Management Policy outlines the processes to	Inspected the Vulnerability and Patch Management Policy to determine that the company has established the processes for	No exceptions noted.

	procedures that put policies into action.	efficiently respond to identified vulnerabilities.	vulnerability management including scan requirements and remediation strategies.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Business Continuity and Disaster Recovery Policy governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Inspected the Business Continuity and Disaster Recovery Policy to determine that the recovery stage begins with the restoration of the company's services in an available commercial cloud provider's region, for Engineering.	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.	A Data Retention and Disposal Policy specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement.	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.	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected the Change Management Policy to determine that a policy is in place which governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes. Observed the policy acceptance data for the company's Change Management Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	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.	A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Inspected the Performance Review Policy to determine that a policy is in place which provides personnel context and transparency into their performance and career development processes. Observed the policy acceptance data for the company's Performance Review Policy to determine that all of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	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.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Inspected the Risk Assessment and Treatment Policy to determine that a policy is in place which governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy. Observed the policy acceptance data for the company's Risk Assessment and Treatment Policy to determine that all of the in-scope	No exceptions noted.

			personnel have accepted the policy and that the policy has been approved within the last year.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that the company has defined the minimum device configuration settings, including encryption, passwords, malware protection, and security updates.	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.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control and Termination Policy to determine that a policy governs authentication and access to applicable systems, data, and networks. Observed the policy acceptance data for the company's Access Control and Termination Policy to determine that most of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	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.	Internal personnel review and accept applicable information security policies at least annually.	Inspected the Information Security Policy to determine that internal personnel review and accept applicable information security policies at least annually. Observed the policy acceptance data to determine that the company's policies have been accepted by all of the internal personnel within the last year.	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.	A Data Classification Policy details the security and handling protocols for sensitive data.	Inspected the Data Classification Policy to determine that the company has identified the types of confidential, internal, public, and restricted data that is collected and the processes for labeling, handling, storing, and deleting such information.	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.	A Privacy Policy to both external users and internal personnel. This policy details the company's privacy commitments.	Inspected the privacy policy document to determine that the company has communicated its privacy and security commitments to external users and internal personnel.	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.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents to resolution.	Inspected the Security Incident Response Plan to determine that the company has established an incident response plan that provides guidelines for detecting, reporting, responding, and tracking incidents to resolution.	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.	Information security roles and responsibilities are outlined for personnel responsible for the security, availability, and	Inspected the Internal Control Policy, Performance Review Policy, and Security Incident Response Plan, to determine that the information security responsibilities of the senior management, managers, and the security response team have been	No exceptions noted.

		confidentiality of the system.	documented. Inspected a sample of job descriptions for various positions to determine that the company outlines the roles and responsibilities in relevant job descriptions.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy to determine that a Network Security Policy is in place which identifies the requirements for protecting information and systems within and across networks. Observed the policy acceptance data for the company's Network Security Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	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.	An Acceptable Use Policy defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools and internet access.	Inspected the Acceptable Use Policy to determine that the company has defined the standards for appropriate and secure use of hardware and electronic systems including storage media, communication tools, and internet access.	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.	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected the Secure Development Policy to determine that a policy is in place which defines the requirements for secure software and system development and maintenance. Observed the policy acceptance data for the company's Secure Development Policy to determine that all of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	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.	A Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	Inspected the Code of Conduct to determine that the company has defined ethical expectations against business standards and the consequences of violating these standards.	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.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy to determine that the company manages and maintains its internal controls through the use of the Secureframe platform. Observed that the company uses Secureframe to continuously monitor its internal security controls and SOC 2 security controls have owners.	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.	An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	Inspected the Encryption and Key Management Policy to determine that the company has defined the guidelines and requirements for data encryption and cryptographic key management.	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.	An Information Security Policy establishes the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	Inspected the Information Security Policy to determine that the company has established requirements to maintain a secure information security posture.	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.	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy to determine that the company has defined the guidelines to maintain the internal control system and to protect its assets, stating that it uses Secureframe to manage and maintain its internal controls.	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.	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected the Secure Development Policy to determine that a policy is in place which defines the requirements for secure software and system development and maintenance. Observed the policy acceptance data for the company's Secure Development Policy to determine that all of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	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.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to grant users administrative access to the production infrastructure based on the principle of least privilege. Observed the list of AWS IAM users and user access tracking to determine that the no-user access list and tracking is tested during the audit period. Inspected the AWS resource data to determine that AWS S3 buckets permission is granted via ACL and the root account is not used for day-to-day account management.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to grant users administrative access to the production infrastructure based on the principle of least privilege.	No exceptions noted.



	assets to protect them from security events to meet the entity's objectives.		Observed the list of AWS IAM users and user access tracking to determine that the no-user access list and tracking is tested during the audit period. Inspected the AWS resource data to determine that AWS S3 buckets permission is granted via ACL and the root account is not used for day-to-day account management.	
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.	Upon termination or when internal personnel no longer require access, system access is removed, as applicable.	Inspected the Access Control and Termination Policy to determine that the IT/Engineering team is required to revoke access of terminated employees for systems and applications within 24 hours of their last day with the company or sooner if necessary. Observed implemented termination checklist to determine that upon termination or when internal personnel no longer require access, system access is removed, as applicable.	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.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control and Termination Policy to determine that a policy governs authentication and access to applicable systems, data, and networks. Observed the policy acceptance data for the company's Access Control and Termination Policy to determine that most of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	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.	Configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	Inspected the Network Security Policy to determine that the company is required to configure firewalls and restrict networking ports and protocols based on the principle of least functionality. Observed that all application load balancers have WAF enabled to determine that networking services and environments are restricted as necessary. Inspected the AWS resource data to determine that AWS EC2 security groups are configured for least functionality, AWS S3 buckets are configured to restrict static website hosting, AWS EKS clusters are configured to enable private endpoint settings, AWS SageMaker notebook instance is configured to disable direct internet access, AWS S3 buckets are configured to restrict public access, CloudTrail logs access is restricted, AWS ElasticSearch domain is configured to enable VPC endpoint,	No exceptions noted.

			AWS SNS topics are configured to restrict global send or subscribe, and AWS Lambda policy is configured to prevent access from the public. Observed the separate accounts used for development and production environments to determine that segregation between development, and production environments is established.	
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.	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected the Network Security Policy to determine that the company is required to use monitoring solutions to detect network-based threats and generate alerts. Observed the Grafana dashboard showing various metrics being monitored to determine that the company uses Grafana to monitor its cloud infrastructure. Inspected an internal Slack channel showing an automated message from AlertManager notifying the company of an issue in AWS to determine that monitoring and alerting are enabled on the company's infrastructure. Observed the company's WAF rules in Cloudflare to determine that WAFs are utilized by the company. Observed that GuardDuty is enabled for all accounts and AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch to determine that security tools have been implemented by the company to provide monitoring of network traffic to the production environment.	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.	An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	Inspected the Encryption and Key Management Policy to determine that the company has defined the guidelines and requirements for data encryption and cryptographic key management.	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	Service data is encrypted-at-rest.	Inspected the Encryption and Key Management Policy to determine that the company is required to use the NIST protocols for data encryption at rest. Inspected the AWS resource data to determine that AWS RDS instances, EFS volumes, RDS snapshots, SSM parameters, EBS snapshots,	No exceptions noted.

	meet the entity's objectives.		Athena workgroups, and ElasticSearch domains are configured to be encrypted at rest.	
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.	Access to, erasure of, or destruction of customer data is restricted to personnel that need access based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to provide users unique access keys and restrict access to systems and applications based on the principle of least privilege. Inspected the AWS resource data to determine that AWS IAM policies are not connected directly to user accounts, AWS EC2 instances require associated keys for password-less secure shell (SSH) login, and the AWS root account has limited usage. Inspected a list of device data to determine that the company settings are configured to enforce hard drive encryption for each connected device.	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.	Non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	Inspected the Access Control and Termination Policy to determine that the company is required to provide users unique access keys and restrict access to systems and applications based on the principle of least privilege. Inspected the AWS resource data to determine that AWS EC2 instances require associated keys for password-less secure shell (SSH) login and monitoring of AWS canary-token access key activity is 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.	Company endpoints are managed and configured with anti-virus, and hard drive encryption.	Inspected the Configuration and Asset Management Policy to determine that the company requires user endpoint storage to be encrypted, malware protection to be enabled, and passwords to be of at least 8 characters and be complex. Observed that all relevant endpoints managed with Kolide have anti-malware software installed and hard drive encryption enabled to determine that company endpoints are configured with anti-virus and hard drive encryption. Inspected the Security and Privacy settings of a macOS device showing that FileVault is enabled to determine that company endpoints have hard drive encryption enabled.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them	Development, staging, and production environments are segregated.	Inspected the Information Security Policy to determine that the company is required to maintain controls for the segregation of development and production environments. Inspected a list of separate folders for	No exceptions noted.

	from security events to meet the entity's objectives.		development and production to determine that development, staging, and production environments are segregated.	
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.	Personnel are assigned unique IDs to access sensitive systems, networks, and information.	Inspected the Access Control and Termination Policy to determine that the company is required to provide users with unique credentials to access systems and applications. Observed the personnel list maintained on Secureframe to determine that all personnel have been assigned unique emails.	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.	Personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	Inspected the Access Control and Termination Policy to determine that the company requires its personnel to use unique and complex passwords with at least 8 characters, and use MFA to access the company email, version control tool, and cloud infrastructure. Inspected the password policy for AWS IAM to determine that the passwords are to be configured for at least 10 characters, with uppercase and lowercase letters, at least one number, and a symbol. Inspected the employee MFA status data to determine that MFA is enabled on Heroku, Cloudflare, AWS, and Google Workspace.	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.	A list of system assets, components, and respective owners are maintained and reviewed at least annually.	Inspected the Configuration and Asset Management Policy to determine that the company is required to maintain an inventory of servers, desktops, laptops, and other devices used to store, create, modify, delete, or transmit confidential information. Inspected lists of user endpoints, AWS resources, and GitHub and Bitbucket repositories along with assigned owners to determine that the company maintains an inventory of system assets, components, and respective owners.	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.	Descriptions of the company's services and systems are available to both internal personnel and external users.	Inspected the network diagram to determine that the company provides a description of its workflow to internal users. Inspected the company's website to determine that a description of services and systems has been provided to external users.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes	System owners conduct scheduled user access reviews of production servers, databases, and	Inspected the Access Control and Termination Policy to determine that quarterly reviews of access rights are to be performed.	No exceptions noted.

	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.	applications to validate internal user access is commensurate with job responsibilities.	Observed access review meeting snapshots to determine that system owners conduct scheduled user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	
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.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control and Termination Policy to determine that a policy governs authentication and access to applicable systems, data, and networks. Observed the policy acceptance data for the company's Access Control and Termination Policy to determine that most of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	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.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to grant users administrative access to the production infrastructure based on the principle of least privilege. Observed the list of AWS IAM users and user access tracking to determine that the no-user access list and tracking is tested during the audit period. Inspected the AWS resource data to determine that AWS S3 buckets permission is granted via ACL and the root account is not used for day-to-day account management.	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.	Upon termination or when internal personnel no longer require access, system access is removed, as applicable.	Inspected the Access Control and Termination Policy to determine that the IT/Engineering team is required to revoke access of terminated employees for systems and applications within 24 hours of their last day with the company or sooner if necessary. Observed implemented termination checklist to determine that upon termination or when internal personnel no longer require access, system access is removed, as applicable.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes	Non-console access to production infrastructure is restricted to users with	Inspected the Access Control and Termination Policy to determine that the company is required to provide users unique access keys and restrict access to systems and applications	No exceptions noted.

	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.	a unique SSH key or access key.	based on the principle of least privilege. Inspected the AWS resource data to determine that AWS EC2 instances require associated keys for password-less secure shell (SSH) login and monitoring of AWS canary-token access key activity is enabled.	
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.	Personnel are assigned unique IDs to access sensitive systems, networks, and information.	Inspected the Access Control and Termination Policy to determine that the company is required to provide users with unique credentials to access systems and applications. Observed the personnel list maintained on Secureframe to determine that all personnel have been assigned unique emails.	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.	Access to, erasure of, or destruction of customer data is restricted to personnel that need access based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to provide users unique access keys and restrict access to systems and applications based on the principle of least privilege. Inspected the AWS resource data to determine that AWS IAM policies are not connected directly to user accounts, AWS EC2 instances require associated keys for password-less secure shell (SSH) login, and the AWS root account has limited usage. Inspected a list of device data to determine that the company settings are configured to enforce hard drive encryption for each connected device.	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.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to grant users administrative access to the production infrastructure based on the principle of least privilege. Observed the list of AWS IAM users and user access tracking to determine that the no-user access list and tracking is tested during the audit period. Inspected the AWS resource data to determine that AWS S3 buckets permission is granted via ACL and the root account is not used for day-to-day account management.	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.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control and Termination Policy to determine that a policy governs authentication and access to applicable systems, data, and networks. Observed the policy acceptance data for the company's Access Control and Termination Policy to determine that most of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	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.	Personnel are assigned unique IDs to access sensitive systems, networks, and information.	Inspected the Access Control and Termination Policy to determine that the company is required to provide users with unique credentials to access systems and applications. Observed the personnel list maintained on Secureframe to determine that all personnel have been assigned unique emails.	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.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to grant users administrative access to the production infrastructure based on the principle of least privilege. Observed the list of AWS IAM users and user access tracking to determine that the no-user access list and tracking is tested during the audit period. Inspected the AWS resource data to determine that AWS S3 buckets permission is granted via ACL and the root account is not used for day-to-day account management.	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.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to grant users administrative access to the production infrastructure based on the principle of least privilege. Observed the list of AWS IAM users and user access tracking to determine that the no-user access list and tracking is tested during the audit period. Inspected the AWS resource data to determine that AWS S3 buckets permission is granted via	No exceptions noted.

			ACL and the root account is not used for day-to-day account management.	
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.	Access to, erasure of, or destruction of customer data is restricted to personnel that need access based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to provide users unique access keys and restrict access to systems and applications based on the principle of least privilege. Inspected the AWS resource data to determine that AWS IAM policies are not connected directly to user accounts, AWS EC2 instances require associated keys for password-less secure shell (SSH) login, and the AWS root account has limited usage. Inspected a list of device data to determine that the company settings are configured to enforce hard drive encryption for each connected device.	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.	System owners conduct scheduled user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	Inspected the Access Control and Termination Policy to determine that quarterly reviews of access rights are to be performed. Observed access review meeting snapshots to determine that system owners conduct scheduled user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	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.	Upon termination or when internal personnel no longer require access, system access is removed, as applicable.	Inspected the Access Control and Termination Policy to determine that the IT/Engineering team is required to revoke access of terminated employees for systems and applications within 24 hours of their last day with the company or sooner if necessary. Observed implemented termination checklist to determine that upon termination or when internal personnel no longer require access, system access is removed, as applicable.	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	Non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	Inspected the Access Control and Termination Policy to determine that the company is required to provide users unique access keys and restrict access to systems and applications based on the principle of least privilege. Inspected the AWS resource data to determine that AWS EC2 instances require associated keys for password-less secure shell (SSH) login	No exceptions noted.

	concepts of least privilege and segregation of duties, to meet the entity's objectives.		and monitoring of AWS canary-token access key activity is enabled.	
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.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control and Termination Policy to determine that a policy governs authentication and access to applicable systems, data, and networks. Observed the policy acceptance data for the company's Access Control and Termination Policy to determine that most of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to grant users administrative access to the production infrastructure based on the principle of least privilege. Observed the list of AWS IAM users and user access tracking to determine that the no-user access list and tracking is tested during the audit period. Inspected the AWS resource data to determine that AWS S3 buckets permission is granted via ACL and the root account is not used for day-to-day account management.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to grant users administrative access to the production infrastructure based on the principle of least privilege. Observed the list of AWS IAM users and user access tracking to determine that the no-user access list and tracking is tested during the audit period. Inspected the AWS resource data to determine that AWS S3 buckets permission is granted via ACL and the root account is not used for day-to-day account management.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to	Upon termination or when internal personnel no longer require access, system access is removed, as applicable.	Inspected the Access Control and Termination Policy to determine that the IT/Engineering team is required to revoke access of terminated employees for systems and applications within 24 hours of their last day with the company or sooner if necessary. Observed implemented termination checklist to determine that upon termination or when	No exceptions noted.

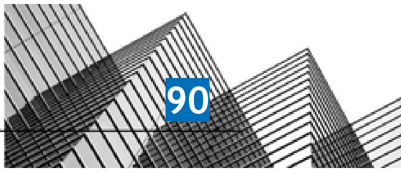
	meet the entity's objectives.		internal personnel no longer require access, system access is removed, as applicable.	
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that the company has defined the minimum device configuration settings, including encryption, passwords, malware protection, and security updates.	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.	Upon customer request, Company requires that data that is no longer needed from databases and other file stores is removed in accordance with agreed-upon customer.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement. Observed open search dashboard to determine that upon customer request, Company requires that data that is no longer needed from databases and other file stores is removed in accordance with agreed-upon customer.	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.	Procedures are in place to retain customer data based on agreed-upon customer requirements or in line with information security policies.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement.	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.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that the company has defined the minimum device configuration settings, including encryption, passwords, malware protection, and security updates.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	Inspected the Network Security Policy to determine that the company is required to configure firewalls and restrict networking ports and protocols based on the principle of least functionality. Observed that all application load balancers have WAF enabled to determine that networking services and environments are	No exceptions noted.

			restricted as necessary. Inspected the AWS resource data to determine that AWS EC2 security groups are configured for least functionality, AWS S3 buckets are configured to restrict static website hosting, AWS EKS clusters are configured to enable private endpoint settings, AWS SageMaker notebook instance is configured to disable direct internet access, AWS S3 buckets are configured to restrict public access, CloudTrail logs access is restricted, AWS ElasticSearch domain is configured to enable VPC endpoint, AWS SNS topics are configured to restrict global send or subscribe, and AWS Lambda policy is configured to prevent access from the public. Observed the separate accounts used for development and production environments to determine that segregation between development, and production environments is established.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy to determine that a Network Security Policy is in place which identifies the requirements for protecting information and systems within and across networks. Observed the policy acceptance data for the company's Network Security Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	Inspected the Access Control and Termination Policy to determine that the company requires its personnel to use unique and complex passwords with at least 8 characters, and use MFA to access the company email, version control tool, and cloud infrastructure. Inspected the password policy for AWS IAM to determine that the passwords are to be configured for at least 10 characters, with uppercase and lowercase letters, at least one number, and a symbol. Inspected the employee MFA status data to determine that MFA is enabled on Heroku, Cloudflare, AWS, and Google Workspace.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from	Procedures are in place to retain customer data based on agreed-upon customer requirements or	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the	No exceptions noted.

	sources outside its system boundaries.	in line with information security policies.	customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	Inspected the Encryption and Key Management Policy to determine that the company has defined the guidelines and requirements for data encryption and cryptographic key management.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Service data transmitted over the internet is encrypted-in-transit.	Inspected the Encryption and Key Management Policy to determine that the company is required to use strong security protocols such as TLS 1.3 or at a minimum, TLS 1.1 protocol to encrypt the data transmitted over the Internet. Inspected the security certificate of the company's website which is valid until September 7, 2023, to determine that the company encrypts data in transit. Inspected the AWS resource data to determine that AWS ElasticSearch domains are configured to use node-to-node encryption and enforce HTTPS connections.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected the Network Security Policy to determine that the company is required to use monitoring solutions to detect network-based threats and generate alerts. Observed the Grafana dashboard showing various metrics being monitored to determine that the company uses Grafana to monitor its cloud infrastructure. Inspected an internal Slack channel showing an automated message from AlertManager notifying the company of an issue in AWS to determine that monitoring and alerting are enabled on the company's infrastructure. Observed the company's WAF rules in Cloudflare to determine that WAFs are utilized by the company. Observed that GuardDuty is enabled for all accounts and AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch to determine that security tools have been implemented by the company to	No exceptions noted.

			provide monitoring of network traffic to the production environment.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control and Termination Policy to determine that a policy governs authentication and access to applicable systems, data, and networks. Observed the policy acceptance data for the company's Access Control and Termination Policy to determine that most of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Descriptions of the company's services and systems are available to both internal personnel and external users.	Inspected the network diagram to determine that the company provides a description of its workflow to internal users. Inspected the company's website to determine that a description of services and systems has been provided to external users.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.	Inspected the Information Security Policy to determine that the company is required to collect and monitor audit logs and alerts, and is required to use logging solutions or SIEM tools to collect event information. Observed a list of logged events in Elastic to determine that logging and monitoring software is utilized by the company. Observed the Grafana dashboard showing various metrics being monitored to determine that the company uses Grafana to monitor its cloud infrastructure. Inspected an internal Slack channel showing an automated message from AlertManager notifying the company of an issue to determine that monitoring and alerting are enabled on the company's infrastructure. Observed that AWS RDS logs are ingested in CloudWatch, AWS EC2 security groups are configured for least functionality, AWS VPC flow logs are enabled, AWS Application load balancers have access logging enabled, CloudTrail is enabled for all regions within an account, log file integrity validation is enabled in CloudWatch, AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch, S3 buckets storing CloudTrail logs have server access logs enabled, GuardDuty is enabled for all accounts, AWS OpenSearch Service logs are published to CloudWatch, AWS	No exceptions noted.

			CloudTrail is integrated with CloudWatch, AWS EKS logs are sent to CloudWatch, and most of the AWS S3 buckets have server access logs enabled.	
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.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to grant users administrative access to the production infrastructure based on the principle of least privilege. Observed the list of AWS IAM users and user access tracking to determine that the no-user access list and tracking is tested during the audit period. Inspected the AWS resource data to determine that AWS S3 buckets permission is granted via ACL and the root account is not used for day-to-day account management.	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.	An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	Inspected the Encryption and Key Management Policy to determine that the company has defined the guidelines and requirements for data encryption and cryptographic key management.	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.	Access to, erasure of, or destruction of customer data is restricted to personnel that need access based on the principle of least privilege.	Inspected the Access Control and Termination Policy to determine that the company is required to provide users unique access keys and restrict access to systems and applications based on the principle of least privilege. Inspected the AWS resource data to determine that AWS IAM policies are not connected directly to user accounts, AWS EC2 instances require associated keys for password-less secure shell (SSH) login, and the AWS root account has limited usage. Inspected a list of device data to determine that the company settings are configured to enforce hard drive encryption for each connected device.	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	Service data is encrypted-at-rest.	Inspected the Encryption and Key Management Policy to determine that the company is required to use the NIST protocols for data encryption at rest. Inspected the AWS resource data to determine that AWS RDS instances, EFS volumes, RDS snapshots, SSM parameters, EBS snapshots,	No exceptions noted.



	meet the entity’s objectives.		Athena workgroups, and ElasticSearch domains are configured to be encrypted at rest.	
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.	Company endpoints are managed and configured with anti-virus, and hard drive encryption.	Inspected the Configuration and Asset Management Policy to determine that the company requires user endpoint storage to be encrypted, malware protection to be enabled, and passwords to be of at least 8 characters and be complex. Observed that all relevant endpoints managed with Kolide have anti-malware software installed and hard drive encryption enabled to determine that company endpoints are configured with anti-virus and hard drive encryption. Inspected the Security and Privacy settings of a macOS device showing that FileVault is enabled to determine that company endpoints have hard drive encryption enabled.	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.	Service data transmitted over the internet is encrypted-in-transit.	Inspected the Encryption and Key Management Policy to determine that the company is required to use strong security protocols such as TLS 1.3 or at a minimum, TLS 1.1 protocol to encrypt the data transmitted over the Internet. Inspected the security certificate of the company's website which is valid until September 7, 2023, to determine that the company encrypts data in transit. Inspected the AWS resource data to determine that AWS ElasticSearch domains are configured to use node-to-node encryption and enforce HTTPS connections.	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.	Procedures are in place to retain customer data based on agreed-upon customer requirements or in line with information security policies.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement.	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	An Acceptable Use Policy defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools and internet access.	Inspected the Acceptable Use Policy to determine that the company has defined the standards for appropriate and secure use of hardware and electronic systems including storage media, communication tools, and internet access.	No exceptions noted.

	meet the entity's objectives.			
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.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that the company has defined the minimum device configuration settings, including encryption, passwords, malware protection, and security updates.	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.	Production data is not used in the development and testing environments, unless required for debugging customer issues.	Inspected the Secure Development Policy to determine that confidential and restricted data, as well as data that can be related to individual persons, should not be used as test data, and exceptions may be approved only by Oded Messer, in which case Oded Messer should define how such test data are protected. Observed AWS databases to determine that production data is not used in the development and testing environments, unless required for debugging customer issues.	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.	A list of system assets, components, and respective owners are maintained and reviewed at least annually.	Inspected the Configuration and Asset Management Policy to determine that the company is required to maintain an inventory of servers, desktops, laptops, and other devices used to store, create, modify, delete, or transmit confidential information. Inspected lists of user endpoints, AWS resources, and GitHub and Bitbucket repositories along with assigned owners to determine that the company maintains an inventory of system assets, components, and respective owners.	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.	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected the Change Management Policy to determine that a policy is in place which governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes. Observed the policy acceptance data for the company's Change Management Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	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.	Development, staging, and production environments are segregated.	Inspected the Information Security Policy to determine that the company is required to maintain controls for the segregation of development and production environments. Inspected a list of separate folders for development and production to determine that	No exceptions noted.

			development, staging, and production environments are segregated.	
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.	Company endpoints are managed and configured with anti-virus, and hard drive encryption.	Inspected the Configuration and Asset Management Policy to determine that the company requires user endpoint storage to be encrypted, malware protection to be enabled, and passwords to be of at least 8 characters and be complex. Observed that all relevant endpoints managed with Kolide have anti-malware software installed and hard drive encryption enabled to determine that company endpoints are configured with anti-virus and hard drive encryption. Inspected the Security and Privacy settings of a macOS device showing that FileVault is enabled to determine that company endpoints have hard drive encryption enabled.	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.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected the Configuration and Asset Management Policy to determine that the company requires production systems handling confidential data to have documented baseline configurations. Inspected details of cryptographic keys used in different scopes to determine that baseline settings and/or vendor documentation are utilized for configuring cloud services or on-premise servers.	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.	System changes are approved by at least 1 independent person prior to deployment into production.	Inspected the Change Management Policy to determine that system changes must be approved by at least 1 independent person prior to deployment into production. Inspected the repositories to determine that code changes are documented and tracked through GitHub and independent approvals for significant infrastructure changes are required to determine that system changes must be approved by at least 1 independent person prior to deployment into production.	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.	An Acceptable Use Policy defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools and internet access.	Inspected the Acceptable Use Policy to determine that the company has defined the standards for appropriate and secure use of hardware and electronic systems including storage media, communication tools, and internet access.	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.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company has established an incident response plan that provides guidelines for detecting, reporting, responding, and tracking incidents to resolution.	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.	A 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Inspected the Vulnerability and Patch Management Policy to determine that the company schedules third party security assessments and penetration tests at least annually. Observed performed penetration test to determine that a 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	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.	A Vulnerability Management and Patch Management Policy outlines the processes to efficiently respond to identified vulnerabilities.	Inspected the Vulnerability and Patch Management Policy to determine that the company has established the processes for vulnerability management including scan requirements and remediation strategies.	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.	Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.	Inspected the Information Security Policy to determine that the company is required to collect and monitor audit logs and alerts, and is required to use logging solutions or SIEM tools to collect event information. Observed a list of logged events in Elastic to determine that logging and monitoring software is utilized by the company. Observed the Grafana dashboard showing various metrics being monitored to determine that the company uses Grafana to monitor its cloud infrastructure. Inspected an internal Slack channel showing an automated message from AlertManager notifying the company of an issue to determine that monitoring and alerting are enabled on the company's infrastructure. Observed that AWS RDS logs are ingested in CloudWatch, AWS EC2 security groups are	No exceptions noted.

			configured for least functionality, AWS VPC flow logs are enabled, AWS Application load balancers have access logging enabled, CloudTrail is enabled for all regions within an account, log file integrity validation is enabled in CloudWatch, AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch, S3 buckets storing CloudTrail logs have server access logs enabled, GuardDuty is enabled for all accounts, AWS OpenSearch Service logs are published to CloudWatch, AWS CloudTrail is integrated with CloudWatch, AWS EKS logs are sent to CloudWatch, and most of the AWS S3 buckets have server access logs enabled.	
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.	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy to determine that the company requires software changes to be tested in the staging environment before release to production. Inspected the testing data showing that code integration, dependency, and static application security testing is performed in GitHub to determine that software changes are tested prior to being deployed into production.	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.	Alerting software is used to notify impacted teams of potential security events.	Inspected the Network Security Policy to determine that the company has described the requirements and procedures to ensure network and data security. Inspected details of an alert communicated by the Alertmanager to determine that alerting software is used to notify impacted teams of potential security events.	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.	System tools monitors for uptime and availability based on predetermined criteria.	Observed that load balancers are utilized in AWS and Heroku, AWS EC2 instances are monitored in accordance with a set threshold, and AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch to determine that system tools are utilized to monitor for uptime and availability.	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.	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected the Change Management Policy to determine that a policy is in place which governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes. Observed the policy acceptance data for the company's Change Management Policy to determine that all of the relevant employees	No exceptions noted.

			have accepted the policy and that the policy has been approved within the last year.	
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.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected the Configuration and Asset Management Policy to determine that the company requires production systems handling confidential data to have documented baseline configurations. Inspected details of cryptographic keys used in different scopes to determine that baseline settings and/or vendor documentation are utilized for configuring cloud services or on-premise servers.	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.	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected the Network Security Policy to determine that the company is required to use monitoring solutions to detect network-based threats and generate alerts. Observed the Grafana dashboard showing various metrics being monitored to determine that the company uses Grafana to monitor its cloud infrastructure. Inspected an internal Slack channel showing an automated message from AlertManager notifying the company of an issue in AWS to determine that monitoring and alerting are enabled on the company's infrastructure. Observed the company's WAF rules in Cloudflare to determine that WAFs are utilized by the company. Observed that GuardDuty is enabled for all accounts and AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch to determine that security tools have been implemented by the company to provide monitoring of network traffic to the production environment.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that the company has defined the minimum device configuration settings, including encryption, passwords, malware protection, and security updates.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result	A list of system assets, components, and respective owners are maintained and reviewed at least annually.	Inspected the Configuration and Asset Management Policy to determine that the company is required to maintain an inventory of servers, desktops, laptops, and other devices used to store, create, modify, delete,	No exceptions noted.

	in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		or transmit confidential information. Inspected lists of user endpoints, AWS resources, and GitHub and Bitbucket repositories along with assigned owners to determine that the company maintains an inventory of system assets, components, and respective owners.	
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.	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected the Vulnerability and Patch Management Policy to determine that the company performs vulnerability scans periodically. Inspected a list of common vulnerabilities to determine that vulnerability scans are performed on applicable internal infrastructure. Inspected a list of images scanned for vulnerabilities on Sysdig Secure platform to determine that external vulnerability scans are performed on internet-facing infrastructure. Inspected to determine that security vulnerabilities and threats are tracked to resolution, as per applicable SLAs.	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 Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company has established an incident response plan that provides guidelines for detecting, reporting, responding, and tracking incidents to resolution.	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.	Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.	Inspected the Information Security Policy to determine that the company is required to collect and monitor audit logs and alerts, and is required to use logging solutions or SIEM tools to collect event information. Observed a list of logged events in Elastic to determine that logging and monitoring software is utilized by the company. Observed the Grafana dashboard showing various metrics being monitored to determine that the company uses Grafana to monitor its cloud infrastructure.	No exceptions noted.

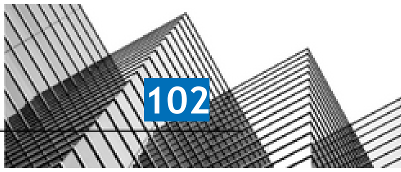
			Inspected an internal Slack channel showing an automated message from AlertManager notifying the company of an issue to determine that monitoring and alerting are enabled on the company's infrastructure. Observed that AWS RDS logs are ingested in CloudWatch, AWS EC2 security groups are configured for least functionality, AWS VPC flow logs are enabled, AWS Application load balancers have access logging enabled, CloudTrail is enabled for all regions within an account, log file integrity validation is enabled in CloudWatch, AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch, S3 buckets storing CloudTrail logs have server access logs enabled, GuardDuty is enabled for all accounts, AWS OpenSearch Service logs are published to CloudWatch, AWS CloudTrail is integrated with CloudWatch, AWS EKS logs are sent to CloudWatch, and most of the AWS S3 buckets have server access logs enabled.	
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.	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected the Network Security Policy to determine that the company is required to use monitoring solutions to detect network-based threats and generate alerts. Observed the Grafana dashboard showing various metrics being monitored to determine that the company uses Grafana to monitor its cloud infrastructure. Inspected an internal Slack channel showing an automated message from AlertManager notifying the company of an issue in AWS to determine that monitoring and alerting are enabled on the company's infrastructure. Observed the company's WAF rules in Cloudflare to determine that WAFs are utilized by the company. Observed that GuardDuty is enabled for all accounts and AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch to determine that security tools have been implemented by the company to provide monitoring of network traffic to the production environment.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of	A continuous monitoring solution monitors internal controls used in the achievement of service	Inspected the Internal Control Policy to determine that the company manages and maintains its internal controls through the use of the Secureframe platform.	No exceptions noted.

	malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	commitments and system requirements.	Observed that the company uses Secureframe to continuously monitor its internal security controls and SOC 2 security controls have owners.	
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.	System tools monitors for uptime and availability based on predetermined criteria.	Observed that load balancers are utilized in AWS and Heroku, AWS EC2 instances are monitored in accordance with a set threshold, and AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch to determine that system tools are utilized to monitor for uptime and availability.	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.	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy to determine that a Network Security Policy is in place which identifies the requirements for protecting information and systems within and across networks. Observed the policy acceptance data for the company's Network Security Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	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.	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inspected the Security Incident Response Plan to determine that the company requires its security response team (SRT) to document, assess, and respond to security incidents according to the incident response process. Inspected details of a resolved security issue on GitHub dashboard to determine that identified incidents are documented, tracked, analyzed, and resolved.	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.	Alerting software is used to notify impacted teams of potential security events.	Inspected the Network Security Policy to determine that the company has described the requirements and procedures to ensure network and data security. Inspected details of an alert communicated by the Alertmanager to determine that alerting software is used to notify impacted teams of potential security events.	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.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company has established an incident response plan that provides guidelines for detecting, reporting, responding, and tracking incidents to resolution.	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.	Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.	Inspected the Information Security Policy to determine that the company is required to collect and monitor audit logs and alerts, and is required to use logging solutions or SIEM tools to collect event information. Observed a list of logged events in Elastic to determine that logging and monitoring software is utilized by the company. Observed the Grafana dashboard showing various metrics being monitored to determine that the company uses Grafana to monitor its cloud infrastructure. Inspected an internal Slack channel showing an automated message from AlertManager notifying the company of an issue to determine that monitoring and alerting are enabled on the company's infrastructure. Observed that AWS RDS logs are ingested in CloudWatch, AWS EC2 security groups are configured for least functionality, AWS VPC flow logs are enabled, AWS Application load balancers have access logging enabled, CloudTrail is enabled for all regions within an account, log file integrity validation is enabled in CloudWatch, AWS metric filters to detect malicious activity in CloudTrail logs are sent to CloudWatch, S3 buckets storing CloudTrail logs have server access logs enabled, GuardDuty is enabled for all accounts, AWS OpenSearch Service logs are published to CloudWatch, AWS CloudTrail is integrated with CloudWatch, AWS EKS logs are sent to CloudWatch, and most of the AWS S3 buckets have server access logs enabled.	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	Production data is not used in the development and testing environments, unless required for debugging customer issues.	Inspected the Secure Development Policy to determine that confidential and restricted data, as well as data that can be related to individual persons, should not be used as test data, and exceptions may be approved only by Oded Messer, in which case Oded Messer should define how such test data are	No exceptions noted.

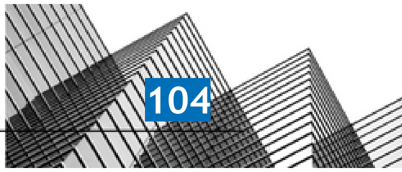
	so, takes actions to prevent or address such failures.		protected. Observed AWS databases to determine that production data is not used in the development and testing environments, unless required for debugging customer issues.	
CC7.3	The entity evaluates security events to determine whether they could 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.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that the company has defined the minimum device configuration settings, including encryption, passwords, malware protection, and security updates.	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.	A Privacy Policy to both external users and internal personnel. This policy details the company's privacy commitments.	Inspected the privacy policy document to determine that the company has communicated its privacy and security commitments to external users and internal personnel.	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.	Terms of Service or the equivalent are published or shared to external users.	Inspected the Terms and Conditions and MSA template to determine that the user agreement and service commitments are communicated to internal personnel and external users.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The Incident Response Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Incident Response Plan based on the test results.	Inspected the Security Incident Response Plan to determine that the company is required to test its Incident Response Plan annually using tabletop exercises and walkthroughs. Inspected a security tabletop exercise to determine that the incident response plan is periodically tested via tabletop exercises.	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.	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected the Vulnerability and Patch Management Policy to determine that the company performs vulnerability scans periodically. Inspected a list of common vulnerabilities to determine that vulnerability scans are performed on applicable internal infrastructure.	No exceptions noted.

			Inspected a list of images scanned for vulnerabilities on Sysdig Secure platform to determine that external vulnerability scans are performed on internet-facing infrastructure. Inspected to determine that security vulnerabilities and threats are tracked to resolution, as per applicable SLAs.	
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.	Terms of Service or the equivalent are published or shared to external users.	Inspected the Terms and Conditions and MSA template to determine that the user agreement and service commitments are communicated to internal personnel and external users.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Alerting software is used to notify impacted teams of potential security events.	Inspected the Network Security Policy to determine that the company has described the requirements and procedures to ensure network and data security. Inspected details of an alert communicated by the Alertmanager to determine that alerting software is used to notify impacted teams of potential security events.	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.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company has established an incident response plan that provides guidelines for detecting, reporting, responding, and tracking incidents to resolution.	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.	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inspected the Security Incident Response Plan to determine that the company requires its security response team (SRT) to document, assess, and respond to security incidents according to the incident response process. Inspected details of a resolved security issue on GitHub dashboard to determine that identified incidents are documented, tracked, analyzed, and resolved.	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.	A 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Inspected the Vulnerability and Patch Management Policy to determine that the company schedules third party security assessments and penetration tests at least annually. Observed performed penetration test to determine that a 3rd party is engaged to conduct a network and application penetration test of the production environment at least	No exceptions noted.

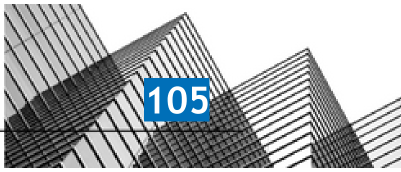


			annually. Critical and high-risk findings are tracked through resolution.	
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy to determine that the company requires software changes to be tested in the staging environment before release to production. Inspected the testing data showing that code integration, dependency, and static application security testing is performed in GitHub to determine that software changes are tested prior to being deployed into production.	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.	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Inspected the Information Security Policy, Code of Conduct, and Acceptable Use Policy to determine that the disciplinary actions including termination of employment against violation of security policies and procedures have been described.	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.	Business Continuity and Disaster Recovery Policy governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Inspected the Business Continuity and Disaster Recovery Policy to determine that the recovery stage begins with the restoration of the company's services in an available commercial cloud provider's region, for Engineering.	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.	After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve company security and operations.	Inspected the Security Incident Response Plan to determine that the company requires its senior management and SRT to prepare a post-mortem report including the key learnings for the prevention of similar incident occurrences in the future. Inspected the lessons learned document which requires a description of the incident, the lessons learned, and the recommended processes that need to be implemented to prevent future incidents to determine that the lessons learned from incidents are required to be documented. No incidents occurred during the observation window.	No exceptions noted. No exceptions noted. No performance
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.	Production data is not used in the development and testing environments, unless required for debugging customer issues.	Inspected the Secure Development Policy to determine that confidential and restricted data, as well as data that can be related to individual persons, should not be used as test data, and exceptions may be approved only by Oded Messer, in which case Oded Messer should define how such test data are protected.	No exceptions noted.

			Observed AWS databases to determine that production data is not used in the development and testing environments, unless required for debugging customer issues.	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inspected the Security Incident Response Plan to determine that the company requires its security response team (SRT) to document, assess, and respond to security incidents according to the incident response process. Inspected details of a resolved security issue on GitHub dashboard to determine that identified incidents are documented, tracked, analyzed, and resolved.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve company security and operations.	Inspected the Security Incident Response Plan to determine that the company requires its senior management and SRT to prepare a post-mortem report including the key learnings for the prevention of similar incident occurrences in the future. Inspected the lessons learned document which requires a description of the incident, the lessons learned, and the recommended processes that need to be implemented to prevent future incidents to determine that the lessons learned from incidents are required to be documented. No incidents occurred during the observation window.	No exceptions noted. No exceptions noted. No performance
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Terms of Service or the equivalent are published or shared to external users.	Inspected the Terms and Conditions and MSA template to determine that the user agreement and service commitments are communicated to internal personnel and external users.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The Business Continuity and Disaster Recovery Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Business Continuity and Disaster Recovery Plan based on the test results.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the company is required to test the plan through tabletop exercises and walkthroughs. Inspected the tabletop exercises held on May 25, 2023, which included test scenarios, the disaster, response, and recovery phases, and the key learnings to determine that the company tests the Business Continuity and Disaster Recovery Plan annually via tabletop exercises.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Backed-up data is restored to a non-production environment at least annually to validate the integrity of backups.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the company requires backups to be periodically tested to ensure that backups are sufficient and reliable.	No exceptions noted.



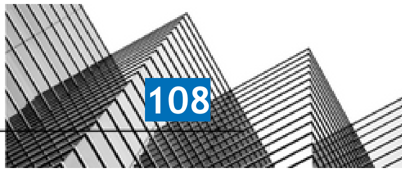
			Inspected a BCP test exercise that included a test scenario and showed an instance restored to a dedicated subdomain to determine that backup restoration testing is performed at the company to validate the integrity of backups.	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The Incident Response Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Incident Response Plan based on the test results.	Inspected the Security Incident Response Plan to determine that the company is required to test its Incident Response Plan annually using tabletop exercises and walkthroughs. Inspected a security tabletop exercise to determine that the incident response plan is periodically tested via tabletop exercises.	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.	System changes are approved by at least 1 independent person prior to deployment into production.	Inspected the Change Management Policy to determine that system changes must be approved by at least 1 independent person prior to deployment into production. Inspected the repositories to determine that code changes are documented and tracked through GitHub and independent approvals for significant infrastructure changes are required to determine that system changes must be approved by at least 1 independent person prior to deployment into production.	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.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy to determine that the company has defined the minimum device configuration settings, including encryption, passwords, malware protection, and security updates.	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.	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected the Secure Development Policy to determine that a policy is in place which defines the requirements for secure software and system development and maintenance. Observed the policy acceptance data for the company's Secure Development Policy to determine that all of the relevant personnel have accepted the policy and that the policy has been approved within the last year.	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.	Production data is not used in the development and testing environments, unless required for debugging customer issues.	Inspected the Secure Development Policy to determine that confidential and restricted data, as well as data that can be related to individual persons, should not be used as test data, and exceptions may be approved only by Oded Messer, in which case Oded Messer should define how such test data are protected.	No exceptions noted.



			Observed AWS databases to determine that production data is not used in the development and testing environments, unless required for debugging customer issues.	
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.	Development, staging, and production environments are segregated.	Inspected the Information Security Policy to determine that the company is required to maintain controls for the segregation of development and production environments. Inspected a list of separate folders for development and production to determine that development, staging, and production environments are segregated.	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.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected the Configuration and Asset Management Policy to determine that the company requires production systems handling confidential data to have documented baseline configurations. Inspected details of cryptographic keys used in different scopes to determine that baseline settings and/or vendor documentation are utilized for configuring cloud services or on-premise servers.	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.	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy to determine that the company requires software changes to be tested in the staging environment before release to production. Inspected the testing data showing that code integration, dependency, and static application security testing is performed in GitHub to determine that software changes are tested prior to being deployed into production.	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.	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected the Vulnerability and Patch Management Policy to determine that the company performs vulnerability scans periodically. Inspected a list of common vulnerabilities to determine that vulnerability scans are performed on applicable internal infrastructure. Inspected a list of images scanned for vulnerabilities on Sysdig Secure platform to determine that external vulnerability scans are performed on internet-facing infrastructure. Inspected to determine that security vulnerabilities and threats are tracked to resolution, as per applicable SLAs.	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.	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected the Change Management Policy to determine that a policy is in place which governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes. Observed the policy acceptance data for the company's Change Management Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	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.	Configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	Inspected the Network Security Policy to determine that the company is required to configure firewalls and restrict networking ports and protocols based on the principle of least functionality. Observed that all application load balancers have WAF enabled to determine that networking services and environments are restricted as necessary. Inspected the AWS resource data to determine that AWS EC2 security groups are configured for least functionality, AWS S3 buckets are configured to restrict static website hosting, AWS EKS clusters are configured to enable private endpoint settings, AWS SageMaker notebook instance is configured to disable direct internet access, AWS S3 buckets are configured to restrict public access, CloudTrail logs access is restricted, AWS ElasticSearch domain is configured to enable VPC endpoint, AWS SNS topics are configured to restrict global send or subscribe, and AWS Lambda policy is configured to prevent access from the public. Observed the separate accounts used for development and production environments to determine that segregation between development, and production environments is established.	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.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inspected minutes of a meeting of the board to determine that the board of directors meets at least annually to review business goals, company initiatives and other internal/external matters. Inspected agenda of a quarterly security meeting to determine that the information security team meets quarterly to discuss security risks and/or other matters as necessary.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Business Continuity and Disaster Recovery Policy governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	Inspected the Business Continuity and Disaster Recovery Policy to determine that the recovery stage begins with the restoration of the company's services in an available commercial cloud provider's region, for Engineering.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan to determine that the company has established an incident response plan that provides guidelines for detecting, reporting, responding, and tracking incidents to resolution.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	A risk register is maintained, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	Inspected the Risk Assessment and Treatment Policy to determine that the company is required to document identified external and internal vulnerabilities and related threats along with risk responses as part of the company's risk assessment. Inspected the risk register which includes risk source, affected assets, vulnerabilities, impact, likelihood, treatment decisions, and residual risk to determine that a risk register is maintained.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners.	Inspected the Risk Assessment and Treatment Policy to determine that a policy is in place which governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	No exceptions noted.



		Risk tolerance and strategies are also defined in the policy.	Observed the policy acceptance data for the company's Risk Assessment and Treatment Policy to determine that all of the in-scope personnel have accepted the policy and that the policy has been approved within the last year.	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment and Treatment Policy to determine that the company is required to perform risk assessments at least annually. Inspected the risk assessment questionnaire, which includes risk categories and responses to specific questions related to diverse risks to determine that the company performs a formal risk assessment annually.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Cybersecurity insurance has been procured to help minimize the financial impact of cybersecurity loss events.	Inspected the Risk Assessment and Treatment Policy to determine that the company may transfer its risk to a third party by purchasing insurance. Inspected the company's cyber liability plus coverage provided by Emrboker showing the insured items and the coverage to determine that the company maintains cybersecurity insurance.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Procedures are in place to retain customer data based on agreed-upon customer requirements or in line with information security policies.	Inspected the Data Retention and Disposal Policy to determine that the company is required to retain data for as long as an account is active or in accordance with the customer agreement unless a different period is required by law whereas data is to be disposed of within 30 days of a request by a customer or in accordance with the agreement.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Inspected the Vendor Management Policy to determine that a policy is in place and defines a framework for the onboarding and management of the vendor relationship lifecycle. Observed the policy acceptance data for the company's Vendor Management Policy to determine that all of the relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.

CC9.2	The entity assesses and manages risks associated with vendors and business partners.	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected the Vendor Management Policy to determine that the company is required to conduct a risk assessment and due diligence for new vendors before engaging with them and a designee is responsible for annual re-reviews of high-risk vendors. Inspected a vendor directory, which shows a list of vendors with their associated risk levels and review dates to determine that vendors are assessed and reviewed annually in accordance with their risk levels. Inspected a master services agreement signed between the company and Lost Rabbit Labs which included confidentiality clauses to determine that the company signs formal agreements with vendors.	No exceptions noted.