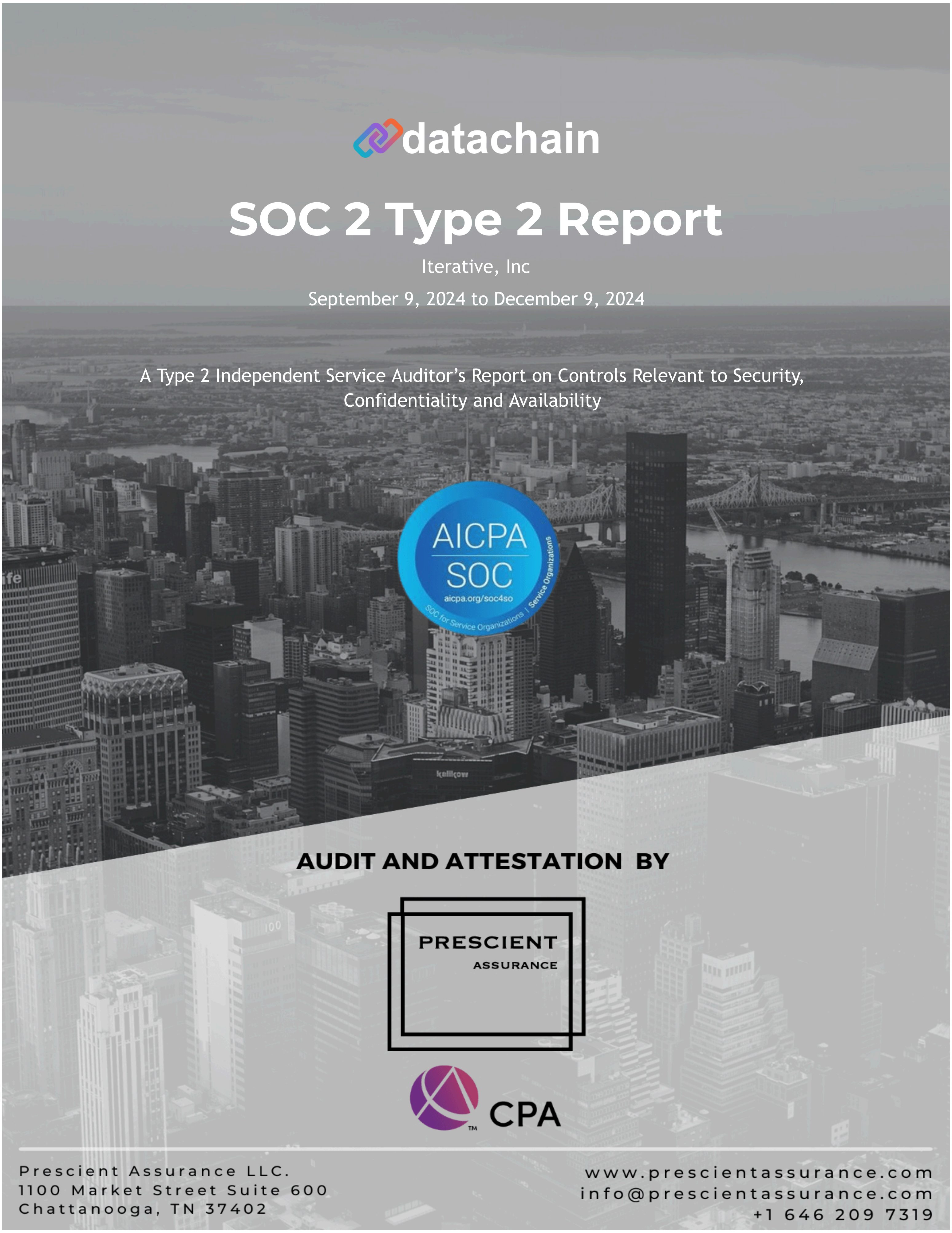


datachain

SOC 2 Type 2 Report

Iterative, Inc

September 9, 2024 to December 9, 2024

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

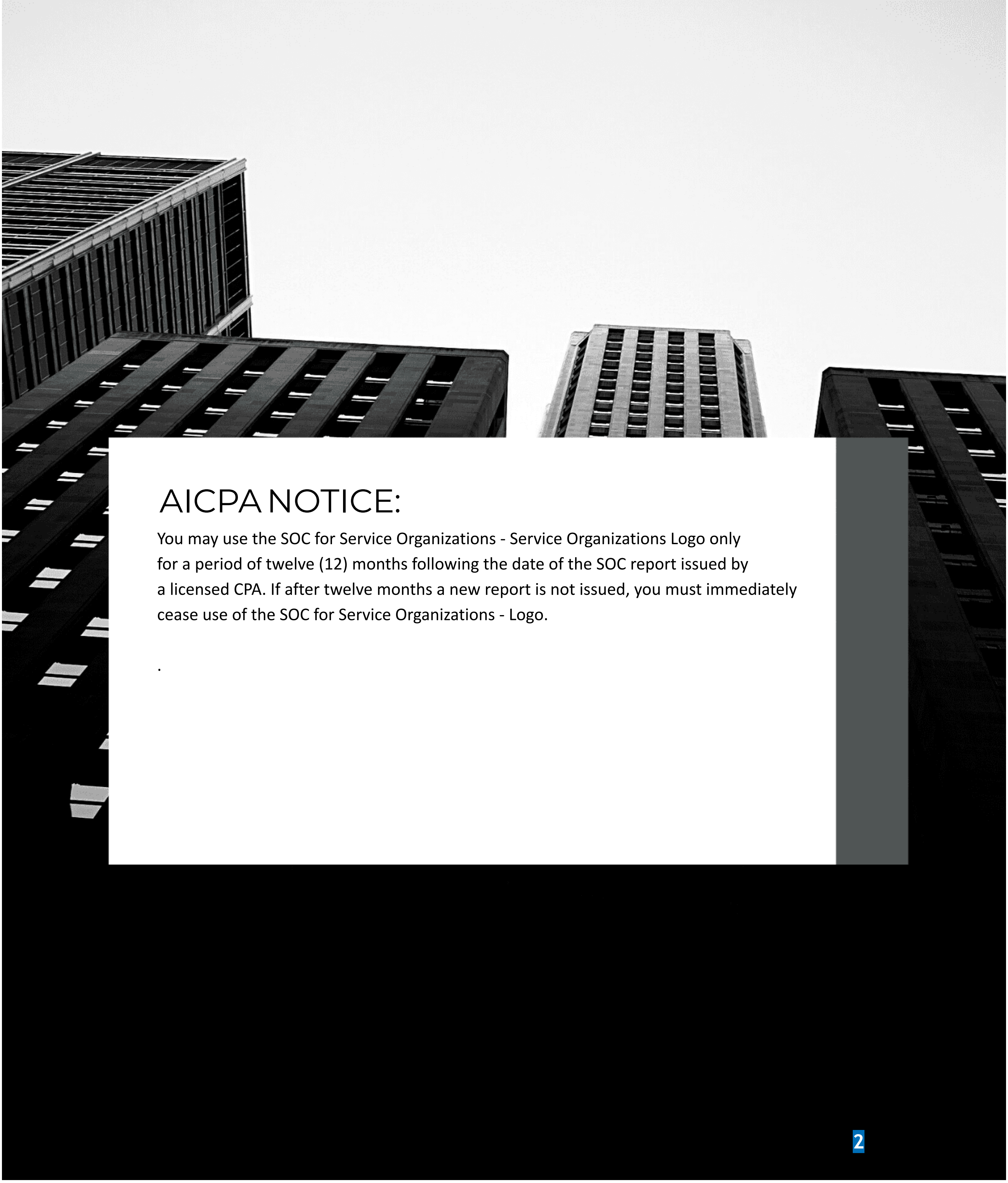
AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA

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

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



AICPA NOTICE:

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

.

Table of Contents

SECTION 1

Management's Assertion

datachain

Management's Assertion

We have prepared the accompanying description of Iterative, Inc's system throughout the period September 9, 2024 to December 9, 2024, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. The description is intended to provide report users with information about 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:

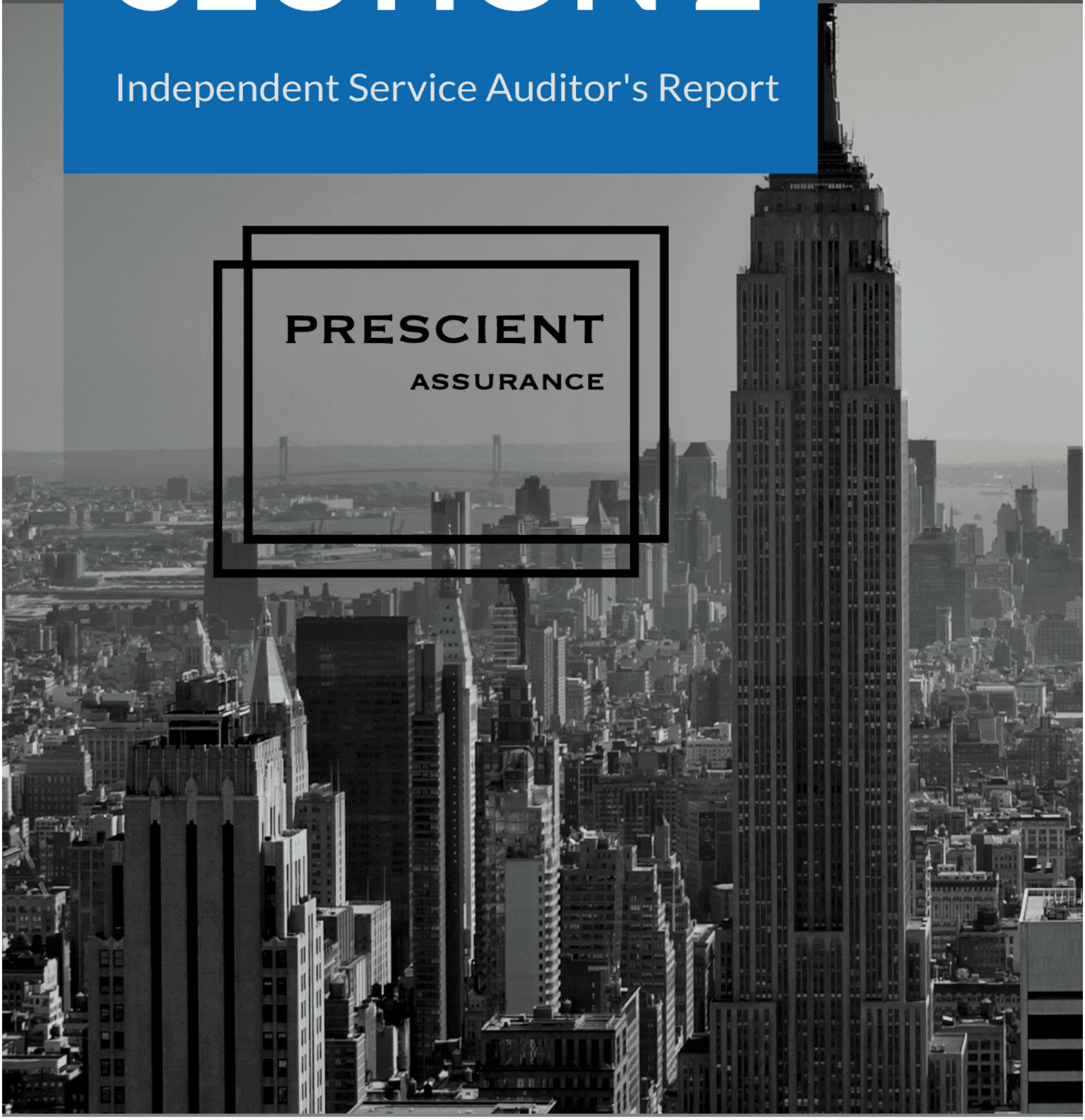
a. The description presents Iterative, Inc's system that was designed and implemented throughout the period September 9, 2024 to December 9, 2024 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period September 9, 2024 to December 9, 2024, 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 September 9, 2024, to December 9, 2024, 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:
Ivan Shcheklein
3BD593A0AF4742D...

Ivan Shcheklein
CTO
Iterative, Inc

SECTION 2

Independent Service Auditor's Report



PRESCIENT ASSURANCE

Independent Service Auditor’s Report

To: Iterative, Inc

Scope

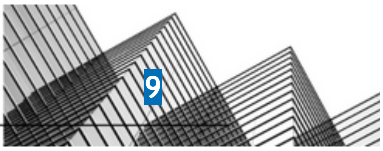
We have examined Iterative, Inc’s (“Iterative, Inc”) accompanying description of its Studio system found in Section 3, titled Iterative, Inc System Description throughout the period September 9, 2024, to December 9, 2024, based on the criteria for a description of a service organization’s system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period September 9, 2024, to December 9, 2024, 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 Auditors' 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 September 9, 2024, to December 9, 2024, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period September 9, 2024, to December 9, 2024, 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 September 9, 2024, to December 9, 2024, 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 September 9, 2024 to December 9, 2024, 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.

Signed by:

Prescient Assurance

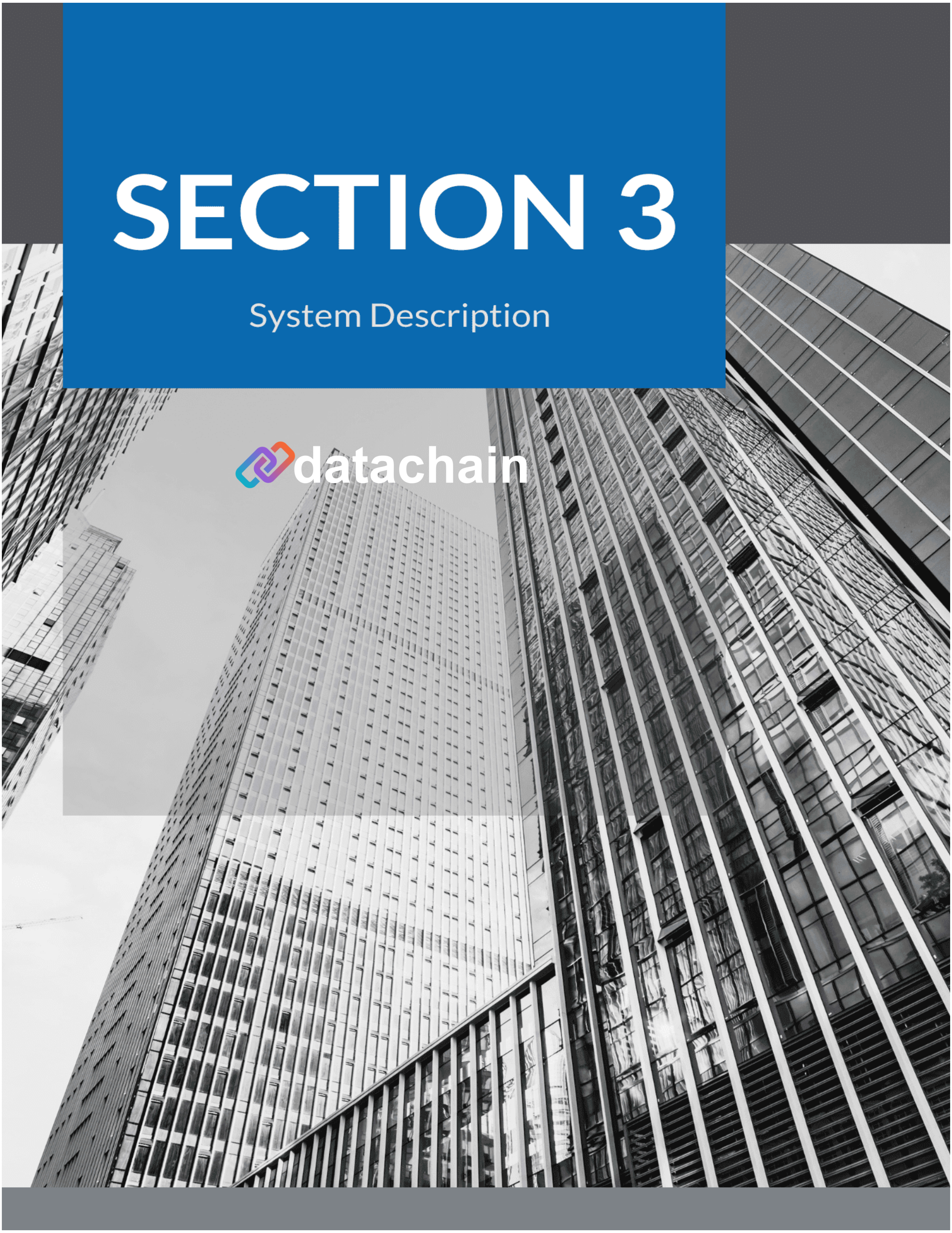
BDAFCCDC4A4A409...

Prescient Assurance LLC
March 25, 2025

SECTION 3

System Description

datachain



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

Company background

Iterative is a leading company in MLOps and AI data processing space, specializing in multimodal and unstructured data. Founded in 2018, the company gained widespread adoption among ML engineers with DVC (Data Version Control), an industry-standard tool for data versioning and reproducibility. It launched its first enterprise SaaS product, Studio, in 2021. Iterative raised a Series A round of $20M in Q2 2021. In 2024, Iterative introduced DataChain, a next-generation platform for multimodal data processing and analytics, which has since become the company's primary focus.

DataChain is a comprehensive AI-powered data platform that enables organizations to manage, query, and analyze multimodal datasets using LLMs and ML models. It extracts metadata with AI, enhances data discoverability, and scales seamlessly. With cloud integration, it offers AI-assisted data curation, provenance tracking, and governance—eliminating redundant copies while ensuring efficiency and security.

DC 2: The Principal Service Commitments and System Requirements

Security commitments

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

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Regular penetration tests over the production environment

Confidentiality commitments

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

- The use of encryption technologies to protect system data both at rest and in transit
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties
- Confidential information must be used only for the purposes explicitly stated in agreements between The Company and user entities

Availability commitments

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

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components
- Responding to customer requests in a reasonably timely manner
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities

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

Iterative maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). To outline the topology of its network and system, the organization maintains the following network and system diagram(s).

3.1 Primary Infrastructure

Hardware	Type	Purpose
Amazon Web Services	Hosting	Outsourced hosting provider
AWS S3	Data Storage	Main storage solution for all services
AWS ECR	ArtifactContainer Registry	Store for container image, helm charts and other packages supporting the platform
AWS EKS	Managed Kubernetes	Scaling and availability of platform resources (containers)
ClickHouse	Data Warehouse	Backend for datasets metadata
AWS ELB	Cloud Networking	Load balancers
AWS VPC	Cloud Networking	Networking layer for services
AWS RDS	Managed database	Managed Postgres for application backend
AWS OpenSearch	Logging	Logs retaining and search
AWS ElastiCache	Caching layer	Services caching storage
Cloudflare	DNS/DNS Proxy, VPN	Externally available DNS and DNS proxy, VPN
GitHub	Issue Tracking System	Project management (software and others) , incident management and support helpdesk
Notion	Documentation Hub	Internal documentation
Grafana	Notification Service	On call management system
Hexometer	Uptime testing	Website monitoring

Hardware	Type	Purpose
Github	CI/CD	Software deployment pipeline control
GitHub	Source Code Management	Code repository for all aspects of the platform
Sentry	Error tracking	Monitor errors on the Iterative platform
Sysdig	Static Code analysis	Security testing before deployment in CI/CD pipeline

3.2 Primary Software:

System/Application	Operating System	Purpose
Amazon Web Services	Linux/Ubuntu	Cloud hosting services
Typescript	Linux	Primary development language/runtime for application front-end
Pyhon	Linux	Primary development language/runtime for application back-end
PostgreSQL	Linux	Transactional database
Redis	Linux	Used to maintain cached data
AWS OpenSearch	N/A	Log aggregator
AWS Cloudwatch	N/A	Monitoring for cloud resources
Prometheus	Linux	Time series monitoring system
Grafana	Linux	Monitoring visualization tool
Kibana	Linux	Logging search tool
Terraform	N/A	Infrastructure as a Code (IaaC) tool
ArgoCD	Linux	Kubernetes Application Deployment and management tool
Helm	N/A	Kubernetes templating tool

3.3 People

Studio Team - Development:

- Manager: Ivan Shcheklein (CTO)
- Fam (Thomas) Kumwar - SW Engineer (Frontend)
- Ranjit (Amrit) Ghimire - SW Engineer (Backend)
- Ivan Longin - SW Engineer (Backend)
- Marcin Jasion - SW Engineer (Platform / Infrastructure)
- Helio Machado - SW Engineer (Platform / Infrastructure)
- Matt Seddon - SW Engineer (Backend / Frontend)

Sales/CSE Teams:

- Manager: Dmitry Petrov (CEO):
- Tibor Mach - Solution Engineer

3.4 Security Processes and Procedures

Secure Development and Maintenance

Access to production systems for maintenance is restricted to authorized employees. Review process, approval procedures of any changes to the production system and deployment ensure secure development.

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 (yearly, last done Dec 2024).
- 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.

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.

Secure Engineering Principles

Ivan Shcheklein 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.

Security Requirements

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

Security Requirements Related to Public Networks

Ivan Shcheklein 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

Ivan Shcheklein 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

Checking and Testing the Implementation of Security Requirements

Ivan Shcheklein 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.

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.

Change Control

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

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 Ivan Shcheklein, in which case Ivan Shcheklein must define how such test data are protected.

Required Security Training

Ivan Shcheklein 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:
Git forge (GitHub, GitLab, Bitbucket, S3) -> Studio app (parsed in memory, cached on local Redis) -> RDS (AWS, isolated network)

3.5 Third Party Access

Key Vendors for Studio app:

- GitHub
- GitLab
- Bitbucket
- S3
- Google Drive
- AWS (EKS, RDS, ELB, CloudTrail logs, OpenSearch)
- Sentry.io
- Plausible
- 1Password - internal password management
- Notion - proposals, documentation
- Slack - instant messaging, operations

3.6 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
- DataChain - FOSS

DC 4: Disclosures about Identified Security Incidents

We've received a security report on Oct 16th 2024 via email stating that the publicly readable API keys we use on our web sites for Algolia are overpermissioned introducing a publicly exploitable persistent cross-site scripting vulnerability. Algolia is a service that doesn't have access to customers or production data and is used only to index open-source documentation and provide search on the DVC website.
An internal ticket was created with the details, actions plan and timeline tracking. The incident was resolved on 2024-10-16 22:37:00. Ivan Shcheklein and the team discussed the steps needed to be taken to improve the security; the team also composed the lessons learned summary and shared it internally. The team also improved security checks to automatically detect publicly published Algolia keys.

No user data was compromised due to this incident.

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 CollaborationAll 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

Eligibility

All employees are provided an annual performance review.

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.

5.3 Management's Philosophy and Operating Style

Iterative's management team is committed to fostering innovation in AI-driven data management while ensuring the highest standards of security, compliance, and operational integrity. As a pioneer in MLOps and AI data processing, Iterative operates at the forefront of multimodal and unstructured data workflows, providing customers with advanced tools for data versioning, analytics, and governance.

The leadership team at Iterative continuously evaluates technological advancements to refine and enhance **DataChain**, our next-generation platform for multimodal data processing. We are dedicated to maintaining the trust our customers place in us by prioritizing data integrity, privacy, and security across all our offerings. As we advance AI-assisted data curation, provenance tracking, and governance, we remain steadfast in our commitment to eliminating redundant data copies while optimizing efficiency and compliance.

The management team convenes regularly to assess emerging trends in AI, machine learning, and regulatory landscapes, ensuring that Iterative's solutions align with evolving industry standards and legal requirements. Any major strategic shifts or product innovations undergo thorough review to confirm their compatibility with our core mission and customer commitments.

Specific control activities implemented to support these objectives include:

- **Board Meetings and Documentation:** The board of directors convenes at least once per year, maintaining formal meeting minutes that document key discussions, decisions, and directives related to cybersecurity, compliance, and operational strategy.
- **Board of Directors bylaws** are established to provide corporate oversight, strategic direction, and governance for the company from a top-down perspective.
- **Security team meetings** are conducted at least quarterly to discuss topics related to security initiatives, network security, management of infrastructure and security risks.

By integrating cutting-edge AI technologies with a strong operational control framework, Iterative ensures that its customers can securely and efficiently manage their data while benefiting from the latest advancements in AI-driven analytics and automation.

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

The platform team manages information security - cloud accounts, system security and infrastructure.
Permissions for AWS production environments are managed using IaC (terraform).
System is monitored and logs are retained in OpenSearch.
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

Summary of our security and privacy policies.

DataChain products collect and use only necessary data to function properly. We retain customer data for as long as an account is active, as needed to provide services to customers, or in accordance with the agreement(s) between DataChain and the customer, unless DataChain is required by law to dispose of it earlier or keep it longer. DataChain does not use any personal information collected in the course of doing business for commercial purposes.

As part of our GitOps philosophy, Studio only takes as much information as necessary from your Git service to display experiments, data sets used, metrics, and hyper parameters. Studio only has access to repositories that customer Git services allow. By default, Studio does not access any of the actual data used across your models. Your data remains protected by your cloud credentials (e.g., AWS login, etc.). You may allow Studio access to storage for additional information to be displayed by Studio, but this is optional. Access controls to repositories may be granularly managed directly through a customer's respective Git service (GitHub app, GitLab admin settings, etc.).

Most of our MLOps solutions are open source and thereby subject to public review. Security related to our open source tools would be managed by the user as our tools are downloaded locally. Users manage their own credentials and security policies across resources like clouds, storage, and Git service. There are logging functionality that send anonymized usage data back to DataChain. Users may opt out of this logging. We'll promptly address any security issues that are brought up by the community. Please let us know at GitHub.

5.8 Personnel Security

Background Check:

Background checks or their equivalent are performed before or promptly after a new hires start date, as permitted by 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:

Personnel complete security awareness training every year.

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:

Personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.

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 an 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 itops) 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 GuardDuty - malware protection
- Logs - collection by custom code (using fluentbit) to OpenSearch, viewed with OpenSearch Dashboards, used for debugging
- Grafana - monitoring infra - EKS clusters, RDS, Redis, OpenSearch, ALB
- Plausible + Mixpanel - analytics
- Cloudflare - DNS, DDoS protection, 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 apps - backed up daily, easy to restore.

5.14 System Account Management

Onboarding and 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 and Platform team

5.15.1 Data Classification

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.

5.15.2 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. Ivan Shcheklein 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.

5.15.3 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:

- 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.
- 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.
- 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.

5.15.4 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 (unless it is part of running the service). We sanitize logs.

5.16 Information and Communications Systems

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

5.17 Data Communication

Storage EBS volumes, RDS, Redis and OpenSearch storage are encrypted with AES-256-GCM keys, K8s Secrets - same
Cloudflare Access
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.

5.18 Monitoring Controls

Pen-test - currently ongoing. Remediation after the initial test is WIP, progress can be tracked.

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 (CSOCs)

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/Google/Azure management.

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

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 availabilities may occur

DC 9: Disclosures Of Significant Changes In Last 1 Year

Changes to the services provided

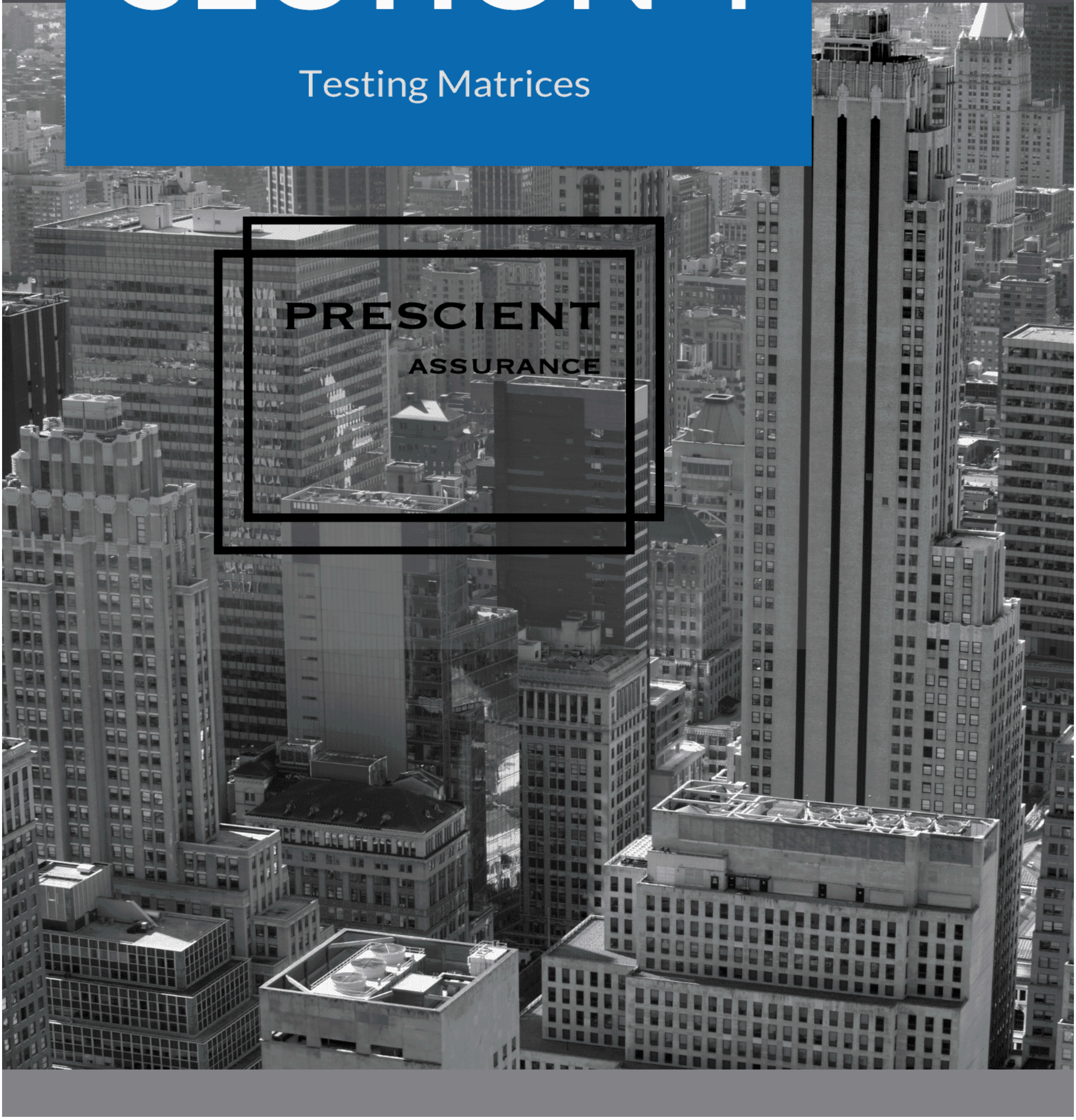
- Launched https://datachain.ai, comprising both an open-source project and a SaaS offering.
- Migrated part of the SaaS cloud infrastructure (batch compute) to Google Cloud.
- Integrated managed batch compute and analytical database services into our SaaS offering.
- Implemented an OpenID Connect Provider as part of our SaaS offering, simplifying access to resources hosted on third-party cloud vendors.
- Implemented SAML authentication for SSO

Significant changes to personnel / organizational structure:

- The team consolidated and people moved from some FOSS to the Studio team.
- Went through headcount reduction in February 2024 - >20% overall. As part of this, we let go of Senior Backend Engineer from the Studio team.

SECTION 4

Testing Matrices



PRESCIENT

ASSURANCE

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

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

Prescient Assurance LLC conducted the examination testing throughout the period September 09, 2024 to December 09, 2024.

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

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

Types of Tests Generally Performed

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

Test Types	Description of Tests
Inquiry	**Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.**
Inspection	**Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following:** ● **Examination / Inspection of source documentation and authorizations to verify transactions processed.** ● **Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures.** ● **Examination / Inspection of systems documentation, configurations, and settings; and** ● **Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.**

Observation	**Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.**
Re-performance	**Re-performed the control to verify the design and / or operation of the control activity as performed if applicable.**

General Sampling Methodology

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

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

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.	The system is configured for high availability to support continuous availability, when applicable.	Inspected the configurations of multiple availability zones, load balancers, and autoscaling groups to determine that the system is configured for high availability and to support continuous 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.	System tools monitors for uptime and availability based on predetermined criteria.	Inspected the load balancer and AWS CloudTrail configurations to determine that system tools are in place for monitoring uptime and availability.	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 completed risk register assessment from the audit period to determine that formal risk assessments are performed, including identifying relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	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.	Inspected the configurations of multiple availability zones, load balancers, and autoscaling groups to determine that the system is configured for high availability and to support continuous 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.	System tools monitors for uptime and availability based on predetermined criteria.	Inspected the load balancer and AWS CloudTrail configurations to determine that system tools are in place for monitoring uptime and availability.	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.	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected the compliance reports and Bridge Letters to confirm that the company's Vendor SOC 2 reports are collected and reviewed 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 infrastructure to meet its objectives.	Full backups are performed and retained in accordance with the Business Continuity and Disaster Recovery Policy.	Inspected the backup configurations to determine that full backups are performed and retained in accordance with the Business Continuity and Disaster Recovery Plan.	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 Backup Restoration test to determine that backed-up data is restored to a non-production environment at least annually to validate the integrity of backups.	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	Inspected the Business Continuity Disaster Recovery Tabletop to determine that a tabletop exercise, covering a power outage scenario, response discussions, and key learnings,	No exceptions noted.

		Recovery Plan based on the test results.	was conducted on 2024-11-07, demonstrating periodic testing and improvements.	
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 Plan to determine that it describes the restoration processes of the services and infrastructure after a disruptive event.	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 a strong password policy, anti-virus, and hard drive encryption	Inspected the password and encryption configurations through Secureframe to determine that the company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	No exceptions noted.
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 user account listing and configurations to determine that access to, erasure of, or destruction of customer data is restricted to personnel that need access based on the principle of least privilege.	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 has developed a Data Retention and Disposal Policy that specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	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 a template of the company's disposal log which includes the instructions for logging the disposal request to determine that the company has processes in place to delete customer data upon receiving a request.	No exceptions noted.
C1.1	The entity identifies and maintains confidential	Business Continuity and Disaster Recovery Policy governs required	Inspected the Business Continuity and Disaster Recovery Plan to	No exceptions noted.

	information to meet the entity's objectives related to confidentiality.	processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.	determine that it describes the restoration processes of the services and infrastructure after a disruptive event.	
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 it describes the security and handling protocols for sensitive data.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Upon customer request, the company requires that data that is no longer needed from databases and other file stores is removed in accordance with agreed-upon customer requirements.	Inspected the data deletion records to determine that upon customer request, the company makes sure that data that is no longer needed from databases and other file stores is removed in accordance with agreed-upon customer requirements.	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 it describes the security and handling protocols for sensitive data.	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 has developed a Data Retention and Disposal Policy that specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	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 a template of the company's disposal log which includes the instructions for logging the disposal request to determine that the company has processes in place to delete customer data upon receiving a request.	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 it includes expectations of good ethical and behavior values, and ramifications of noncompliance.	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	Inquired of the company to determine that no violations of	Not tested because no policy

		disciplinary action is clearly documented in one or more policies.	company policies were reported during the audit period.	violations occurred during the observation window.
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 operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy to determine that the company has developed an Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	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 reviews report, all conducted in June 2024, to determine that formal performance reviews are conducted at least annually.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The 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 board members and information security team to determine that the company has an independent Board of Directors. An information security team has been established to govern cybersecurity.	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 the Board of Directors meeting minutes to determine that the Board of Directors met at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Inspected the security team meeting minutes to determine that the information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results, and other matters as necessary.	No exceptions noted.
CC1.3	Management establishes, with board oversight,	Vendor SOC 2 reports (or equivalent) are collected and	Inspected the compliance reports and Bridge Letters to confirm	No exceptions noted.

	structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	reviewed on at least an annual basis.	that the company's Vendor SOC 2 reports are collected and reviewed annually.	
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities related to security [, availability, processing integrity, confidentiality, and privacy] for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	Inspected a job description to determine that executive roles are outlined in job descriptions and policies, as applicable.	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 and/or other matters as necessary.	Inspected the Board of Directors meeting minutes to determine that the Board of Directors met at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Inspected the security team meeting minutes to determine that the information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results, and other matters as necessary.	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.	Inquired of the company to determine that no new vendors were onboarded during the observation window.	Not tested because no vendors were onboarded during the observation window.
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.	Inspected the organizational chart and employee directory to determine that management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication,	No exceptions noted.

			and publishes the organizational chart to internal personnel.	
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 board members and information security team to determine that the company has an independent Board of Directors. An information security team has been established to govern cybersecurity.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Personnel complete security awareness training every year.	Inspected the completed security awareness training records to determine that personnel complete security awareness training every year.	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.	Inspected the Access Control Policy to determine that 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. Inspected the personnel inventory and inquired with the company to determine that no employees were hired during the audit period.	Not tested because no employees were hired during the audit period.
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 compliance reports and Bridge Letters to confirm that the company's Vendor SOC 2 reports are collected and reviewed annually.	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 reviews report, all conducted in June 2024, to determine that formal performance reviews are conducted at least annually.	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 hire's start date, as permitted by local laws.	Inspected the Access Control Policy to determine that hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill their responsibilities. New hires sign	Not tested because no employees were hired during the audit period.

			confidentiality agreements or equivalents upon hire. Inspected the personnel inventory and inquired with the company to determine that no employees were hired during the audit period.	
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 it includes expectations of good ethical and behavior values, and ramifications of noncompliance.	No exceptions noted.
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 an Information Security Policy establishes the security requirements for maintaining the security, confidentiality, Integrity, and availability of applications, systems, infrastructure, and data.	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 the company has developed a Performance Review Policy that provides personnel context and transparency into their performance and career development process.	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 developed an Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	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.	Inspected the organizational chart and employee directory to determine that management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication,	No exceptions noted.

			and publishes the organizational chart to internal personnel.	
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 Secureframe to determine that a continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	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 the company has developed a Performance Review Policy that provides personnel context and transparency into their performance and career development process.	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 reviews report, all conducted in June 2024, to determine that formal performance reviews are conducted at least annually.	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 the Board of Directors meeting minutes to determine that the Board of Directors met at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Inspected the security team meeting minutes to determine that the information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results, and other matters as necessary.	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 developed an Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and	No exceptions noted.

			encourage adherence to prescribed managerial policies.	
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 to determine that personnel who violate information security policies were subject to disciplinary action and such disciplinary action was clearly documented in one or more policies. No violations of company policies were reported during the audit period.	Not tested because no policy violations occurred during the observation window
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 completed risk register assessment from the audit period to determine that formal risk assessments are performed, including identifying relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	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 an Information Security Policy establishes the security requirements for maintaining the security, confidentiality, Integrity, and availability of applications, systems, infrastructure, and data.	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 Secureframe to determine that a continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	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 report to determine that a third party conducts an annual network and application penetration test of the production environment. No critical or high-risk findings were	No exceptions noted.

			identified during the audit period.	
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 completed vulnerability scanning report and the remediation ticket for a sample of vulnerabilities found to determine that vulnerability scanning is conducted on production infrastructure systems, with identified deficiencies remediated promptly.	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.	Personnel complete security awareness training every year.	Inspected the completed security awareness training records to determine that personnel complete security awareness training every 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 Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy to verify that it outlines the fundamental rules and requirements for network security, ensuring the protection of information within and across networks and supporting information processing facilities.	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 infrastructure architecture and network diagram is maintained.	Inspected an Architecture Diagram to determine that an infrastructure architecture and network diagram is maintained.	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 Management Policy to determine that the plan contains guidelines for the identification, prioritizing, communication, assignment, and tracking of incidents to resolution.	No exceptions noted.
CC2.2	The entity internally communicates information, including	Descriptions of the company's services and systems are available	Inspected the service descriptions published on the company's website to determine	No exceptions noted.

	objectives and responsibilities for internal control, necessary to support the functioning of internal control.	to both internal personnel and external users.	that the description of the company's services and systems are available for internal and external users.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities related to security [, availability, processing integrity, confidentiality, and privacy] for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	Inspected a job description to determine that executive roles are outlined in job descriptions and policies, as applicable.	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.	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 the Board of Directors meeting minutes to determine that the Board of Directors met at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Inspected the security team meeting minutes to determine that the information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results, and other matters as necessary.	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 confidential reporting channel is made available to internal personnel and external parties to report security and other identified concerns.	Inspected the support page and email address for security reporting to determine that the company has made a confidential reporting channel for internal personnel and external parties to report security and other identified concerns.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	A Privacy Policy is established to external users describing the company's privacy commitments.	Inspected the Privacy Policy on the company's website to determine that the company has described its privacy commitments that are conveyed to external users through the website.	No exceptions noted.
CC2.3	The entity communicates with external parties	Senior management and/or board of directors meets at least annually to	Inspected the Board of Directors meeting minutes to determine	No exceptions noted.

	regarding matters affecting the functioning of internal control.	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.	that the Board of Directors met at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Inspected the security team meeting minutes to determine that the information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results, and other matters as necessary.	
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 via the company's website.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Critical information is communicated to external parties, as applicable.	Inspected the Privacy and Cookie Policy and Security and Privacy notification to determine that critical information is communicated to external parties, as applicable.	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 support page and email address for security reporting to determine that the company has made a confidential reporting channel for internal personnel and external parties to report security and other identified concerns.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Descriptions of the company's services and systems are available to both internal personnel and external users.	Inspected the service descriptions published on the company's website to determine that the description of the company's services and systems are available for internal and external users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters	Terms of Service or the equivalent are published or shared to external users.	Inspected the Terms and Conditions and Privacy Policy published on the company's	No exceptions noted.

	affecting the functioning of internal control.		website to determine that the company has shared its service terms with external users.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	An infrastructure architecture and network diagram is maintained.	Inspected an Architecture Diagram to determine that an infrastructure architecture and network diagram is maintained.	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. Reassessment occurs at least annually.	Inspected the Vendor Risk Management Policy and vendor inventory with the last review date to determine that new vendors are assessed according to the policy, including risk assessments and due diligence before engagement, and that annual reassessments are conducted.	Not tested because no vendors were onboarded during the observation window.
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 completed risk register assessment from the audit period to determine that formal risk assessments are performed, including identifying relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	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 the policy describes the procedures for conducting risk assessments and determining appropriate responses.	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,	Inspected the Board of Directors meeting minutes to determine that the Board of Directors met at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.	No exceptions noted.

		controls, changes, audit results and/or other matters as necessary.	Inspected the security team meeting minutes to determine that the information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results, and other matters as necessary.	
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.	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis	Inspected the completed vulnerability scanning report and the remediation ticket for a sample of vulnerabilities found to determine that vulnerability scanning is conducted on production infrastructure systems, with identified deficiencies remediated promptly.	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 the policy describes the procedures for conducting risk assessments and determining appropriate responses.	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.	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 completed risk register assessment from the audit period to determine that formal risk assessments are performed, including identifying relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	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 register to determine that 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.	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.	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 Risk Management Policy and vendor inventory with the last review date to determine that new vendors are assessed according to the policy, including risk assessments and due diligence before engagement, and that annual reassessments are conducted.	Not tested because no vendors were onboarded during the observation window.
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 completed risk register assessment from the audit period to determine that formal risk assessments are performed, including identifying relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	No exceptions noted.
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 completed risk register assessment from the audit period to determine that formal risk assessments are performed, including identifying relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	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 Risk Management Policy and vendor inventory with the last review date to determine that new vendors are assessed according to the policy, including risk assessments and due diligence before engagement, and that annual reassessments are conducted.	Not tested because no vendors were onboarded during the observation window.
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 completed vulnerability scanning report and the remediation ticket for a sample of vulnerabilities found to determine that vulnerability scanning is conducted on production infrastructure	No exceptions noted.

			systems, with identified deficiencies remediated promptly.	
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 report to determine that a third party conducts an annual network and application penetration test of the production environment. No critical or high-risk findings were identified during the audit period.	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 Secureframe to determine that a continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	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.	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 developed an Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	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.	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis	Inspected the completed vulnerability scanning report and the remediation ticket for a sample of vulnerabilities found to determine that vulnerability scanning is conducted on production infrastructure systems, with identified deficiencies remediated promptly.	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	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Secureframe to determine that a continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	No exceptions noted.

	board of directors, as appropriate.			
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 report to determine that a third party conducts an annual network and application penetration test of the production environment. No critical or high-risk findings were identified during the audit period.	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 the Board of Directors meeting minutes to determine that the Board of Directors met at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Inspected the security team meeting minutes to determine that the information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results, and 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 Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Inspected the Vendor Management Policy to ensure it outlines how Iterative executes, manages, and terminates vendor and third-party agreements. Iterative may update this policy periodically to implement varying levels of security controls for different information assets, based on risk and other considerations. The policy is guided by security requirements specific to Iterative, including applicable laws and regulations.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to	Inspected the completed risk register assessment from the audit period to determine that formal risk assessments are	No exceptions noted.

	achievement of objectives to acceptable levels.	security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	performed, including identifying relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	
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, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy to determine that the company has developed an Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	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 the company has developed a Secure Development Policy that defines the requirements for secure software and system development and maintenance.	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 Secureframe to determine that a continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Roles and responsibilities related to security [, availability, processing integrity, confidentiality, and privacy] for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	Inspected a job description to determine that executive roles are outlined in job descriptions and policies, as applicable.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement 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 developed an Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	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 Physical Security Policy that details physical security requirements for the company facilities is in place.	Inspected the Physical Security Policy to determine that the company has a Physical Security Policy that details physical security requirements for the company facilities is in place.	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.	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 to determine that personnel who violate information security policies were subject to disciplinary action and such disciplinary action was clearly documented in one or more policies. No violations of company policies were reported during the audit period.	Not tested because no policy violations occurred during the observation window
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities related to security [, availability, processing integrity, confidentiality, and privacy] for all personnel and executive roles are outlined in job descriptions and policies, as applicable.	Inspected a job description to determine that executive roles are outlined in job descriptions and policies, as applicable.	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 the policy provides a governance structure for authentication and access to applicable systems, data, and networks.	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 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 configurations for new sensitive systems.	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 the company has developed a Change Management Policy that governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	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 it describes the security and handling protocols for sensitive data.	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 has developed a Data Retention and Disposal Policy that specifies how customer data is to be retained and disposed of based on compliance requirements and contractual obligations.	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 Secureframe to determine that a continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	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 policies acknowledgment record for a sample of employees to determine that the internal personnel review and accept applicable information security policies at least annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected the Secure Development Policy to determine that the company has developed a Secure Development Policy that defines the requirements for secure software and system development and maintenance.	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 Vulnerability Management and Patch Management Policy outlines the processes to efficiently respond to identified vulnerabilities.	Inspected the Vulnerability Management and Patch Management Policy to determine that the company has developed a Vulnerability Management and Patch Management Policy that outlines the processes to efficiently respond to identified vulnerabilities.	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 described the cryptographic controls for secure encryption and decryption of app secrets.	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 developed an Internal Control Policy that identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	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 Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy to verify that it outlines the fundamental rules and requirements for network security, ensuring the protection of information within and across networks and supporting information processing facilities.	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 developed an Acceptable Use Policy that defines standards for appropriate and secure use of company 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 Privacy Policy is established to external users describing the company's privacy commitments.	Inspected the Privacy Policy on the company's website to determine that the company has described its privacy commitments that are conveyed to external users through the website.	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 an Information Security Policy establishes the security requirements for maintaining the security, confidentiality,	No exceptions noted.

			Integrity, and availability of applications, systems, infrastructure, and data.	
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 Plan to determine that it describes the restoration processes of the services and infrastructure after a disruptive event.	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 through to resolution.	Inspected the Security Incident Management Policy to determine that the plan contains guidelines for the identification, prioritizing, communication, assignment, and tracking of 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.	A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Inspected the Performance Review Policy to determine that the company has developed a Performance Review Policy that provides personnel context and transparency into their performance and career development process.	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 ensure it outlines how Iterative executes, manages, and terminates vendor and third-party agreements. Iterative may update this policy periodically to implement varying levels of security controls for different information assets, based on risk and other considerations. The policy is guided by security requirements specific to Iterative, including applicable laws and regulations.	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.	Policies and procedures are reviewed and updated by management at least annually.	Inspected the policy review dates to determine that the management reviews and updates company policies and procedures at least annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to	Inspected the Risk Assessment and Treatment Policy to determine that the policy	No exceptions noted.

	expected and in procedures that put policies into action.	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.	describes the procedures for conducting risk assessments and determining appropriate responses.	
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 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 configurations for new sensitive systems.	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 described the cryptographic controls for secure encryption and decryption of app secrets.	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 configurations of the web application firewall, AWS security groups, Cloudtrail firewall, and public access restrictions on S3 buckets to determine that current configurations ensure that access to available networking ports, protocols, services, and environments is restricted.	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 the policy provides a governance structure for authentication and access to applicable systems, data, and networks.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure,	A list of system assets, components, and respective owners are	Inspected the asset inventory to determine that a list of system assets, components, and	No exceptions noted.

	and architectures over protected information assets to protect them from security events to meet the entity's objectives.	maintained and reviewed at least annually.	respective owners were maintained and reviewed at least annually.	
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.	Service data is encrypted-at-rest.	Inspected the automated test data showing that encryption is enabled to determine that service data is encrypted-at-rest.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	Inspected the CloudFlare, GitHub, and 1 password authentication configurations through Seureframe to determine that personnel have strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	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 a strong password policy, anti-virus, and hard drive encryption	Inspected the password and encryption configurations through Secureframe to determine that the company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	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 assigned unique IDs to access sensitive systems, networks, and information.	Inspected personnel data to determine that all employees were assigned unique email IDs to access information systems and networks.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information	Non-console access to production infrastructure is restricted to users with a unique SSH key or access key	Inspected the production authentication configurations and user listings to determine that non-console access to production infrastructure was	No exceptions noted.

	assets to protect them from security events to meet the entity's objectives.		restricted to users with a unique SSH key or access key.	
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.	Users are provisioned access to systems based on the principle of least privilege.	Inspected the production users' listing and configurations to determine that users are provisioned access to systems based on the principle of least privilege.	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.	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 quarterly access review 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.
CC6.2	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 users listing and configurations to determine that administrative access to production infrastructure is restricted based on the principle of least privilege.	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 upon termination or when internal personnel no longer require access, system access is removed, as applicable. Inspected the personnel inventory and inquired with the company to determine that no employees were terminated during the audit period.	Not tested because no employees were terminated during the audit period.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	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 the policy provides a governance structure for authentication and access to applicable systems, data, and networks.	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.	Non-console access to production infrastructure is restricted to users with a unique SSH key or access key	Inspected the production authentication configurations and user listings to determine that non-console access to production infrastructure was restricted to users with a unique SSH key or access key.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information	System owners conduct scheduled user access reviews of production servers, databases, and applications to validate internal user access is	Inspected the quarterly access review to determine that system owners conduct scheduled user access reviews of production servers, databases, and	No exceptions noted.

	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.	commensurate with job responsibilities.	applications to validate internal user access is commensurate with job responsibilities.	
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 upon termination or when internal personnel no longer require access, system access is removed, as applicable. Inspected the personnel inventory and inquired with the company to determine that no employees were terminated during the audit period.	Not tested because no employees were hired during the audit period.
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.	Users are provisioned access to systems based on the principle of least privilege.	Inspected the production users' listing and configurations to determine that users are provisioned access to systems based on the principle of least privilege.	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	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 the policy provides a governance structure for authentication and access to applicable systems, data, and networks.	No exceptions noted.

	concepts of least privilege and segregation of duties, to meet the entity's objectives.			
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.	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected the compliance reports and Bridge Letters to confirm that the company's Vendor SOC 2 reports are collected and reviewed annually.	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.	A Physical Security Policy that details physical security requirements for the company facilities is in place.	Inspected the Physical Security Policy to determine that the company has a Physical Security Policy that details physical security requirements for the company facilities is in place.	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.	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected the compliance reports and Bridge Letters to confirm that the company's Vendor SOC 2 reports are collected and reviewed annually.	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 security tools configurations to determine that security tools are implemented to provide monitoring of network traffic to the production environment.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from	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 described the cryptographic controls for	No exceptions noted.

	sources outside its system boundaries.		secure encryption and decryption of app secrets.	
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 CloudFlare, GitHub, and 1 password authentication configurations through Seureframe to determine that personnel have strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	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 a certificate on the company's website to determine that the company encrypts data while transmitting it over the internet.	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 configurations of the web application firewall, AWS security groups, Cloudtrail firewall, and public access restrictions on S3 buckets to determine that current configurations ensure that access to available networking ports, protocols, services, and environments is restricted.	No exceptions noted.
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 verify that it outlines the fundamental rules and requirements for network security, ensuring the protection of information within and across networks and supporting information processing facilities.	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.	Company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption	Inspected the password and encryption configurations through Secureframe to determine that the company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement,	Service data transmitted over the internet is encrypted-in-transit.	Inspected a certificate on the company's website to determine	No exceptions noted.

	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.		that the company encrypts data while transmitting it over the internet.	
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 is encrypted-at-rest.	Inspected the automated test data showing that encryption is enabled to determine that service data is encrypted-at-rest.	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 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 developed an Acceptable Use Policy that defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access.	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 that the company has securely managed the baseline configurations and codebases for production infrastructure, systems, and applications in cloud services	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 the company has developed a Change Management Policy that governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of	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	No exceptions noted.

	unauthorized or malicious software to meet the entity's objectives.		defined the configurations for new sensitive systems.	
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.	Software changes are tested prior to being deployed into production.	Inspected the tests to determine that software changes are tested prior to being deployed 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 developed an Acceptable Use Policy that defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools, and internet access.	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.	Company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption	Inspected the password and encryption configurations through Secureframe to determine that the company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	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 an AWS, Sentry, and Grafana evidence to determine that the company has deployed logging and monitoring software for monitoring system activity and reporting unusual activity to the management.	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 configurations for new sensitive systems.	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.	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis	Inspected the completed vulnerability scanning report and the remediation ticket for a sample of vulnerabilities found to determine that vulnerability scanning is conducted on production infrastructure systems, with identified deficiencies remediated promptly.	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 report to determine that a third party conducts an annual network and application penetration test of the production environment. No critical or high-risk findings were identified during the audit period.	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 alerting software configurations to determine that the company used alerting software 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.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected that the company has securely managed the baseline configurations and codebases for production infrastructure, systems, and applications in cloud services	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 Management and Patch Management Policy to determine that the company has developed a Vulnerability Management and Patch Management Policy that outlines the processes to efficiently respond to identified vulnerabilities.	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 security tools configurations to determine that security tools are implemented 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 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 an AWS, Sentry, and Grafana evidence to determine that the company has deployed logging and monitoring software for monitoring system activity and reporting unusual activity to the management.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy to verify that it outlines the fundamental rules and requirements for network security, ensuring the protection of information within and across networks and supporting information processing facilities.	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	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected the security tools configurations to determine that security tools are implemented to provide monitoring of network traffic to the production environment.	No exceptions noted.

	whether they represent security events.			
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.	Alerting software is used to notify impacted teams of potential security events.	Inspected the alerting software configurations to determine that the company used alerting software 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 Management Policy to determine that the plan contains guidelines for the identification, prioritizing, communication, assignment, and tracking of 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.	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inspected the track record and lessons learned summary to determine that identified incidents are properly documented, tracked, and analyzed as outlined in the Incident Response Plan.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	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 to determine that personnel who violate information security policies were subject to disciplinary action and such disciplinary action was clearly documented in one or more policies. No violations of company policies were reported during the audit period.	Not tested because no policy violations occurred during the observation window

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 track record and lessons learned summary to determine that identified incidents are properly documented, tracked, and analyzed as outlined in the Incident Response Plan.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Critical information is communicated to external parties, as applicable.	Inspected the Privacy and Cookie Policy and Security and Privacy notification to determine that critical information is communicated to external parties, as applicable.	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 Plan to determine that it describes the restoration processes of the services and infrastructure after a disruptive event.	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 security and operations.	Inspected the lessons learned summary to determine that, after resolving any identified security incident, management provides a "Lessons Learned" document to the team. This document aims to improve security practices and operational efficiency continuously.	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 Management Policy to determine that the plan contains guidelines for the identification, prioritizing, communication, assignment, and tracking of incidents to resolution.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand,	The Incident Response Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes	Inspected the security tabletop exercise report conducted on 23.10.2024 to determine that it included phases such as disaster response, recovery, and key	No exceptions noted.

	contain, remediate, and communicate security incidents, as appropriate.	changes to the Incident Response Plan based on the test results.	learnings, demonstrating periodic testing of the Incident Response Plan and consideration for improvements based on the test results.	
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 track record and lessons learned summary to determine that identified incidents are properly documented, tracked, and analyzed as outlined in the Incident Response Plan.	No exceptions noted.
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 tabletop exercise report conducted on 23.10.2024 to determine that it included phases such as disaster response, recovery, and key learnings, demonstrating periodic testing of the Incident Response Plan and consideration for improvements based on the test results.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Management Policy to determine that the plan contains guidelines for the identification, prioritizing, communication, assignment, and tracking of incidents to resolution.	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 Disaster Recovery Tabletop to determine that a tabletop exercise, covering a power outage scenario, response discussions, and key learnings, was conducted on 2024-11-07, demonstrating periodic testing and improvements.	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 Backup Restoration test to determine that backed-up data is restored to a non-production environment at least annually to validate the integrity of backups.	No exceptions noted.

CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Critical information is communicated to external parties, as applicable.	Inspected the Privacy and Cookie Policy and Security and Privacy notification to determine that critical information is communicated to external parties, as applicable.	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 security and operations.	Inspected the lessons learned summary to determine that, after resolving any identified security incident, management provides a "Lessons Learned" document to the team. This document aims to improve security practices and operational efficiency continuously.	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 the company has developed a Change Management Policy that governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	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.	Development, staging, and production environments are segregated.	Inspected the segregated environments to determine that the company has segregated its development, staging, and production environments.	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 separated test data repositories to determine that the company uses test data for testing purposes.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests,	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected that the company has securely managed the baseline configurations and codebases for production infrastructure,	No exceptions noted.

	approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		systems, and applications in cloud services	
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 configurations for new sensitive systems.	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 tests 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.	Non-console access to production infrastructure is restricted to users with a unique SSH key or access key	Inspected the production authentication configurations and user listings to determine that non-console access to production infrastructure was restricted to users with a unique SSH key or access key.	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 the company has developed a Secure Development Policy that defines the requirements for secure software and system development and maintenance.	No exceptions noted.
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,	Inspected the completed risk register assessment from the audit period to determine that formal risk assessments are performed, including identifying relevant internal and external	No exceptions noted.

		and fraud, and an analysis of risks associated with those threats.	threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	
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. Risk tolerance and strategies are also defined in the policy.	Inspected the Risk Assessment and Treatment Policy to determine that the policy describes the procedures for conducting risk assessments and determining appropriate responses.	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 Management Policy to determine that the plan contains guidelines for the identification, prioritizing, communication, assignment, and tracking of 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 register to determine that 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.	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 cybersecurity insurance certificate to determine that the cybersecurity insurance has been procured to help minimize the financial impact of cybersecurity loss events.	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 Plan to determine that it describes the restoration processes of the services and infrastructure after a disruptive event.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected the compliance reports and Bridge Letters to confirm that the company's Vendor SOC 2 reports are collected and reviewed annually.	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 ensure it outlines how Iterative executes, manages, and terminates vendor and third-party agreements. Iterative may update this policy periodically to implement varying levels of security controls for different information assets, based on risk and other considerations. The policy is guided by security requirements specific to Iterative, including applicable laws and regulations.	No exceptions noted.