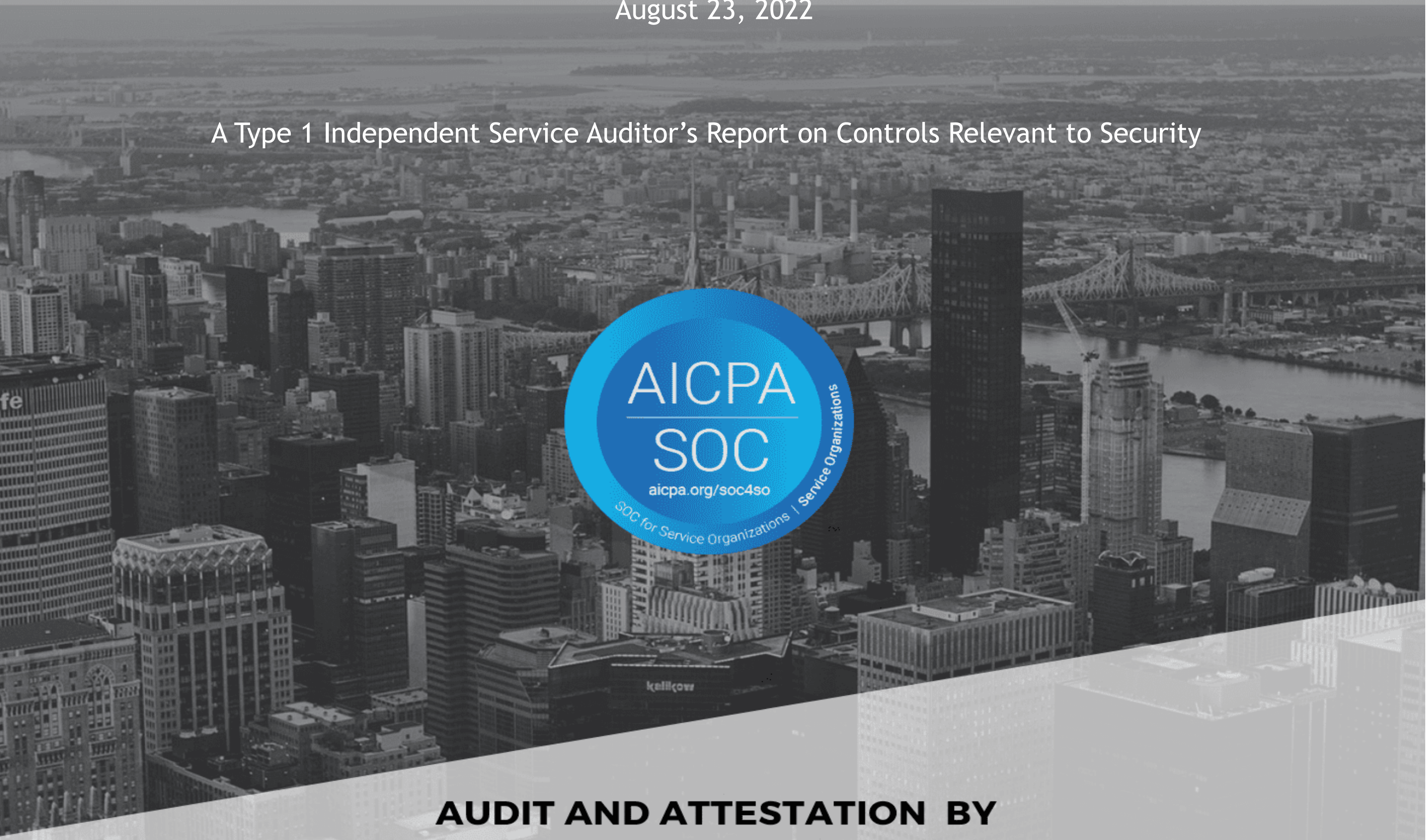
SOC 2 Type 1 Report

Iterative Inc.

August 23, 2022



A Type 1 Independent Service Auditor's Report on Controls Relevant to Security

AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA

Prescient Assurance LLC.
4808 Signal Forest Drive,
Signal Mountain, TN, 37377

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

Table of Contents

Table of Contents 2

Management's Assertion 6

Independent Service Auditor's Report 9

Scope 9

Service Organization's Responsibilities 9

Service Auditors' Responsibilities 10

Inherent Limitations 10

Opinion 11

Restricted Use 11

System Description 13

DC 1: Company Overview and Types of Products and Services Provided 14

DC 2: The Principal Service Commitments and System Requirements 14

DC 3: The Components of the System used to Provide the Services 15

3.1 Primary Infrastructure 15

3.2 Primary Software 16

3.3 People 17

3.4 Security Processes and Procedures 18

Secure Development and Maintenance 18

Secure Engineering Principles 18

Security Requirements Related to Public Networks 18

Checking and Testing the Implementation of Security Requirements 19

Repository and Version Control 19

Change Control 19

Protection of Test 19

Required Security Training 19

3.5 Data 19

3.6 Third Party Access 20

3.7 System Boundaries 20

DC 4: Disclosures about Identified Security Incidents 20

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 20

5.1 Integrity and Ethical Values 20

Equal Opportunity Employment 20

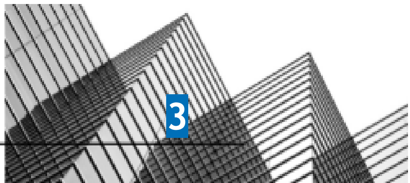
Professionalism 20

Job Duties and Authority 21

Communication and Collaboration 21

Benefits 21

Compliance with Law 21
Conflict of Interest 21
Anti Corruption 21
Gift, Entertainment, Travel & promotional expenditures 22
Internet and Social Media 23
5.2 Commitment to Competence 23
Eligibility 23
Performance Review Schedule 23
Salary Increases 23
Processes 23
5.3 Management's Philosophy and Operating Style 23
5.4 Organizational Structure and Assignment of Authority and Responsibility 23
5.5 Human Resource Policies and Practices 24
Performance Review Schedule 24
Salary Increases 24
Processes 24
5.6 Security Management 24
5.7 Security and Privacy Policies 24
5.8 Personnel Security 25
Background Check 25
Confidentiality 25
Security Awareness 25
System Access Security 25
Account Audits 25
Password Security 25
Rotation Requirements 25
Storing Passwords 25
Acceptable Use 26
Ownership 26
User Responsibilities 26
Personal Use Systems 26
Compliance 26
Remote Work 26
5.9 Physical Security and Environmental Controls 26
5.10 Change Management 27
5.11 System Monitoring 27
5.12 Incident Management 27
5.13 Data Backup and Recovery 27
5.14 System Account Management 27
5.15 Data Classification 28
5.16 Risk Management Responsibilities 28
5.17 Risk Management 28
5.18 Integration with Risk Assessment 29
5.19 Information and Communications 29



5.20 Data Communication 29
5.21 Monitoring Controls 29
DC 6: Complementary User Entity Controls (CUECs) 29
DC 7: Complementary Subservice Organization Controls (CSOCs) 30
DC 8: Disclosures of out of scope Trust Services Criteria 31
DC 9: Disclosure of Significant Changes in Last 1 year 31
Testing Matrices **32**
Tests of Design and Implementation Effectiveness and Results of Tests 33
Scope of Testing 33
Types of Tests Generally Performed 33
Reliability of Information Provided by the Service Organization 34
Test Results 34

SECTION 1

Management's Assertion

iterative

Management's Assertion

We have prepared the accompanying description of Iterative Inc.'s system as of August 23, 2022, 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 and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security 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 as of August 23, 2022, in accordance with the description criteria.

B. The controls stated in the description were suitably designed as of August 23, 2022, 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 as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Iterative Inc.'s controls as of that date.

Dmitry Petrov

CEO of Iterative Inc.

SECTION 2

Independent Service Auditor's Report

Independent Service Auditor’s Report

To: Iterative Inc.

Scope

We have examined Iterative Inc.’s (“Iterative Inc.”) accompanying description of its system as of August 23, 2022, 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 of controls stated in the description as of August 23, 2022, to provide reasonable assurance that Iterative Inc.’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security 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 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 of such 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 design 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 the design 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 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 of controls involves:

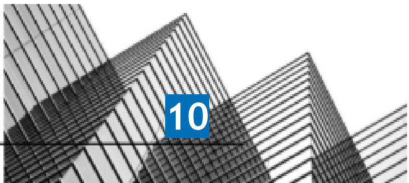
1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
2. Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
3. Performing procedures to obtain 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 and implemented to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
5. 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. The projection to the future of any conclusions about the suitability of the design 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 as of August 23, 2022 in accordance with the description criteria.
B. The controls stated in the description were suitably designed as of August 23, 2022, 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 as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Iterative Inc.'s controls as of that date.

Restricted Use

This report is intended solely for the information and use of Iterative Inc., user entities of Iterative Inc.'s system as of August 23, 2022, 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, and other parties.
3. Internal control and its limitations.
4. Complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Prescient Assurance LLC

John D. Wallace, CPA

Chattanooga, TN

SECTION 3

System Description

iterative

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

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

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

Studio: https://studio.iterative.ai

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

DC 2: The Principal Service Commitments and System Requirements

Principal Service commitments:

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

Trust Service Criteria:

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

Privacy policy:
https://iterative.notion.site/Privacy-Cookie-Policy-edbce9b3b3d14f26950b7dca617b2033

System Requirements:

- Supported browsers - ES6 support required

Major browsers support matrix:

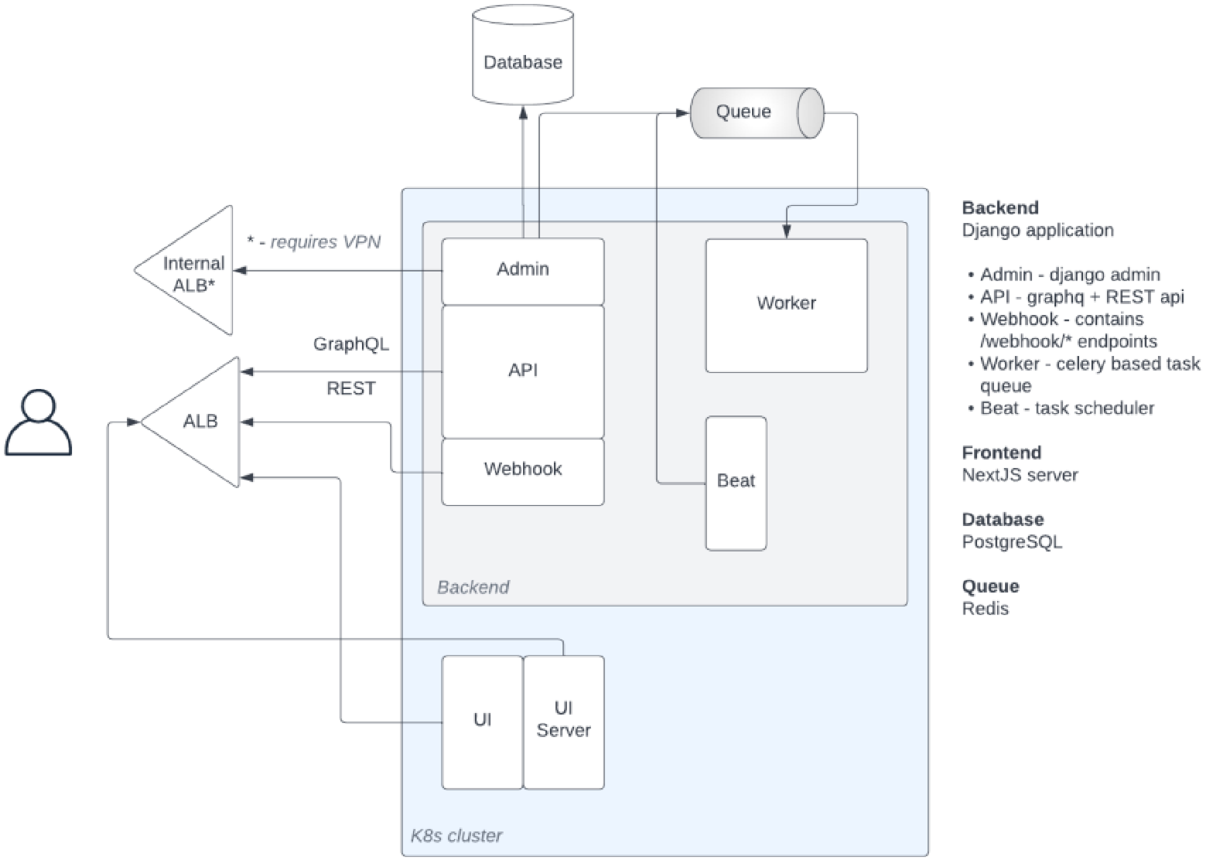
Browser	Version
Chrome	63
Firefox	67
Edge	16
Safari	11.1
Opera	48
Android Browser	104

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

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

3.1 Primary Infrastructure

- System Diagrams:



Backend
Django application

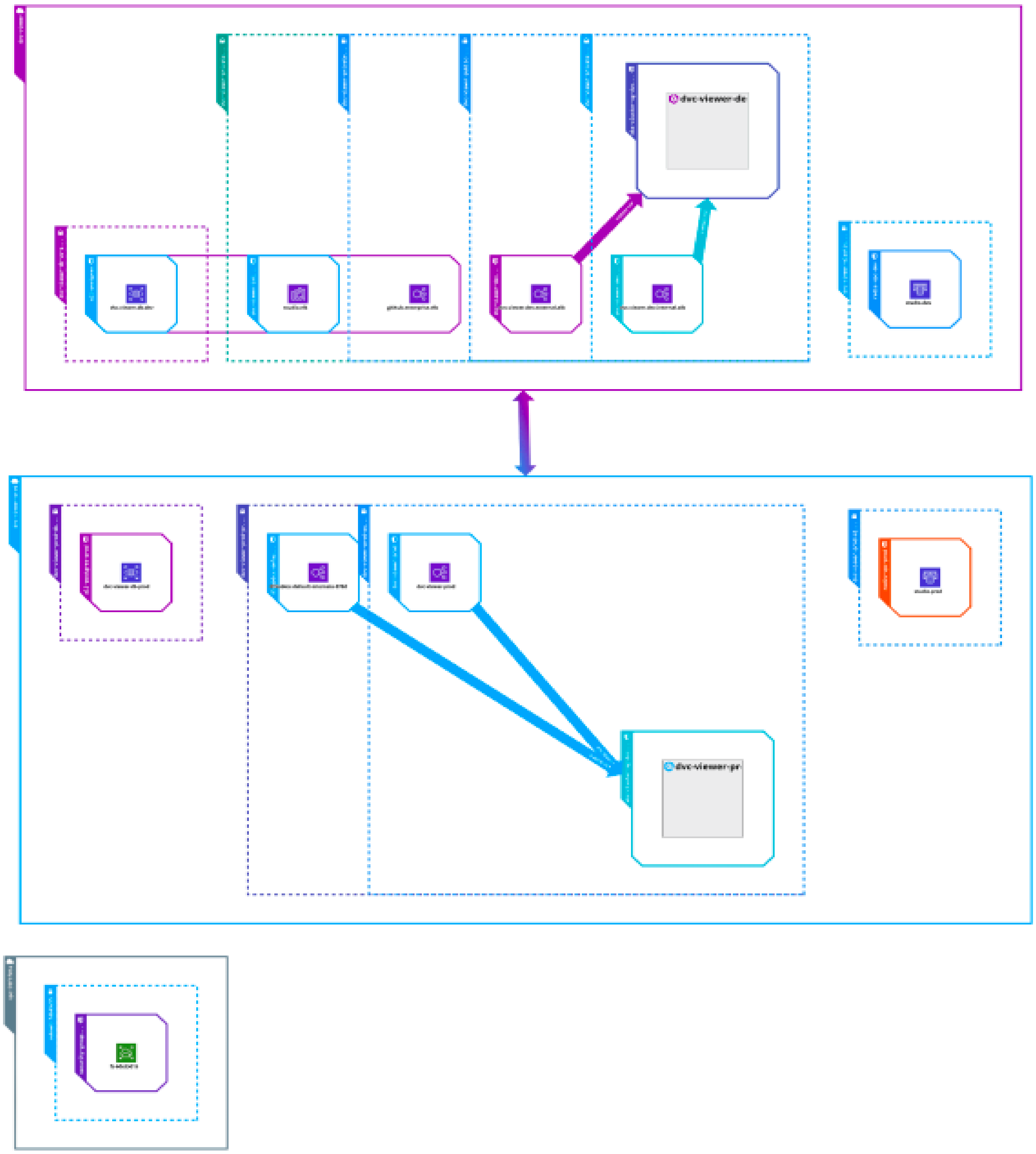
- Admin - django admin
- API - graphq + REST api
- Webhook - contains /webhook/* endpoints
- Worker - celery based task queue
- Beat - task scheduler

Frontend
NextJS server

Database
PostgreSQL

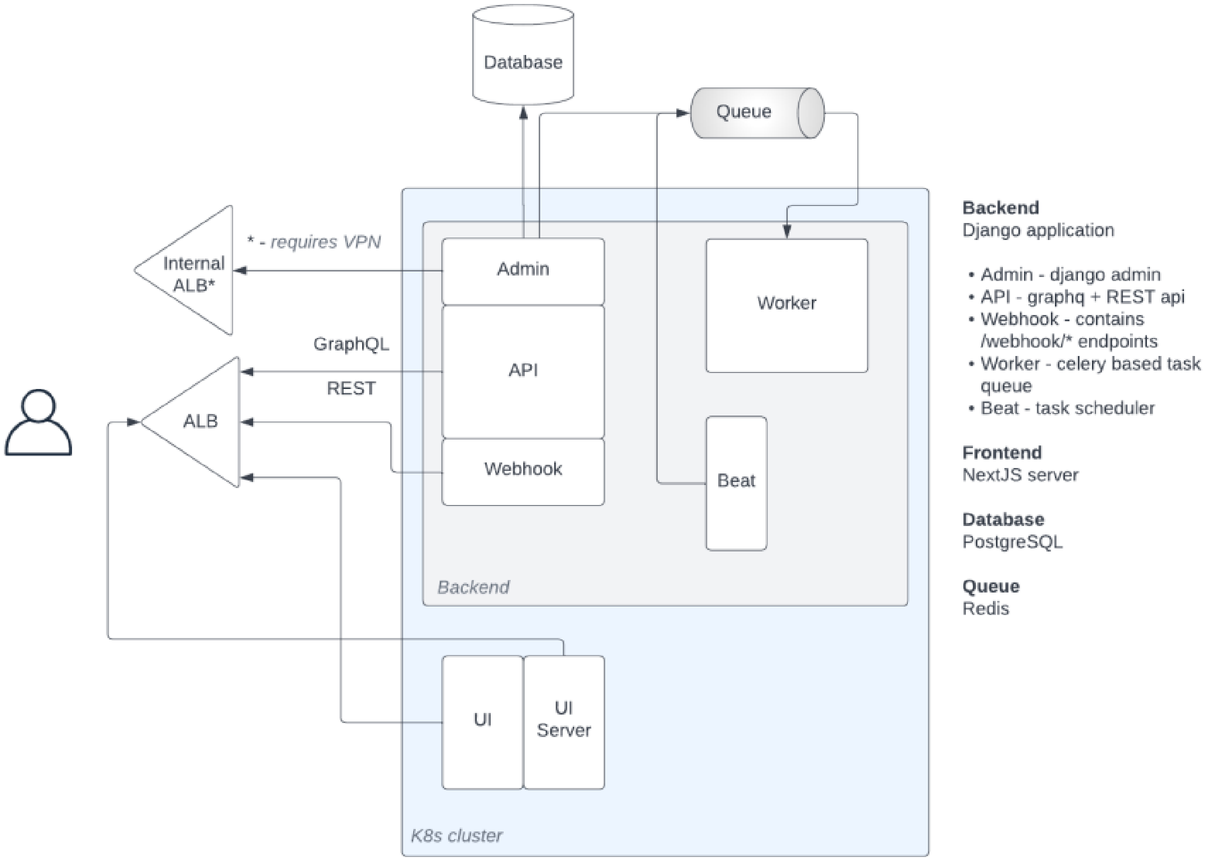
Queue
Redis

- Cloudcraft network diagram



3.2 Primary Software

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



Tech Stack:

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

3.3 People

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

Studio Team - Development:

- Manager: Ivan Shcheklein (CTO)
- Sergey Kryukov - UX Designer

- Manager: Oded Messer (Director of Engineering)
- Sviatlana Sachkouskaya - SW Engineer (Frontend)
- Maksim Shmakov - SW Engineer (Frontend)
- Jelle Bouwman - SW Engineer (Frontend)
- Alex Shchepanovskii - Senior SW Engineer (Backend)
- Ranjit (Amrit) Ghimire - SW Engineer (Backend)
- Guro Bokum - Senior SW Engineer (Backend + Platform / Infra)
- Jesper Svendsen - SW Engineer (Platform / Infra)
- Marcin Jasion - SW Engineer (Platform / Infra)
- Manager: Dmitry Petrov (CEO)
- Tapa Dipti Sitaula - Senior Product Engineer

Sales/CSE Teams:

- Manager: Dmitry Petrov (CEO):
- Mikhail Rozhkov - Customer Success Engineering Manager
- Yura Kasimov - Solution Engineer
- Aleksandr Kolosov - Solution Engineer
- Dan Martinec - Solution Engineer
- Jervis Hui - Director, operations, Go To Market
- Michael (Mike) Moynihan - Account executive
- Charles (Chaz) Black - Account executive
- Alexander Kim - Field Data Scientist

3.4 Security Processes and Procedures

Secure Development and Maintenance

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

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

Security Requirements Related to Public Networks

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

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

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

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

Checking and Testing the Implementation of Security Requirements

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

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 Oded Messer, in which case Oded Messer must define how such test data are protected

Required Security Training

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

3.5 Data

Main flow for user data is very simple:

Git forge (github, gitlab, bitbucket, S3) -> Studio app (parsed in memory, cached on local Redis) -> RDS (AWS, isolated network)

3.6 Third Party Access

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

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

3.7 System Boundaries

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

DC 4: Disclosures about Identified Security Incidents

No incidents identified/disclosed as of date.

DC 5: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved

5.1 Integrity and Ethical Values

Equal Opportunity Employment

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

Professionalism

All employees must show integrity and professionalism in the workplace

Job Duties and Authority

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

Communication and Collaboration

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

Benefits

Iterative expects employees to not abuse their employment benefits.

Compliance with Law

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

Conflict of Interest

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

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

Anti Corruption

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

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

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

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

Gift, Entertainment, Travel & promotional expenditures

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

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

- is reasonable and not extravagant ("of token value" - such as shirts or tote bags that reflect Company's business name and/or logo)
- is appropriate under the circumstances and serves a valid business purpose (e.g. swag in a convention)
- is customary and appropriate under U.S. and local customs;
- is not being offered for any improper purpose, and could not be construed as a bribe, kickback or payoff; no explicit or implicit business interaction is conditioned by it.
- does not violate any company policy;
- does not violate any U.S., local or international laws or regulations; and is accurately described in your expense or other reports and Company's books and records (if gift given). It is essential that Team Members and Partners accurately report expenditures for gifts or entertainment so that the purpose, amount, and recipient of the gift are obvious & transparent to personnel in the company. Expense reports should accurately state the purpose of the expenditures and the identities of the individuals receiving the gifts or entertainment and state whether the gift or entertainment was given to a government employee or official.

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

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

Internet and Social Media

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

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

5.2 Commitment to Competence

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

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

5.4 Organizational Structure and Assignment of Authority and Responsibility

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

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

5.5 Human Resource Policies and Practices

Performance Review Schedule

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

Salary Increases

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

Processes

Management will establish the format and timing of all review processes. The reviews may change from year to year and from person to person. The completed evaluations will be retained and documented. Managers may not discuss any proposed action with the employee until all written approvals are obtained.

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

5.6 Security Management

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

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

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

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

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

5.7 Security and Privacy Policies

Security and Privacy Policy:

https://iterative.ai/security-and-privacy

5.8 Personnel Security

Background Check

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

Confidentiality

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

Security Awareness

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

System Access Security

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

Account Audits

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

Password Security

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

Rotation Requirements

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

Storing Passwords

Passwords must only be stored using 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 CD pipelines that deploys to production instances

5.11 System Monitoring

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

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

5.12 Incident Management

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

5.13 Data Backup and Recovery

RDS is the only storage service that holds a meaningful state for studio apps - backed up daily, easy to restore. No Studio SLAs such as uptime exist today - RDS is auto-recovering but not HA Iterative has plans to move to HA setup (RDS proxy or aurora)

5.14 System Account Management

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

Critical permissions - AWS, are managed by code. Vendor access controls are unified in secureframe . Quarterly Access Control review is being held by Engineering: Director + Platform team

5.15 Data Classification

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

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

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

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

5.16 Risk Management Responsibilities

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

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

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

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

5.17 Risk Management

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

For Fraud/Security risks:

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

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

5.18 Integration with Risk Assessment

Multiple engineers are participating in any decisions affecting control and processes, and risk management (security, efficiency) is 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. We sanitize logs.

5.19 Information and Communications

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

5.20 Data Communication

Storage EBS volumes, RDS, Redis and ES storage are encrypted with AES-256-GCM keys K8s Secrets - same OpenVPN keys use RSA and tls-crypt 2048 bit keys - rotated yearly

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

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

5.21 Monitoring Controls

Pen-test - Completed by LRL (https://www.lostrabbitlabs.com/) on Sep 2022 with no outstanding vulnerabilities found. . Final report can be accessed here: https://drive.google.com/file/d/14k2y9NjzfBObPfMbtzNlGeZfqqGkivaw/view and via secureframe.

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.

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.
CC6.1	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 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	AWS is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2	AWS is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2	AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

DC 8: Disclosures of out of scope Trust Services Criteria

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

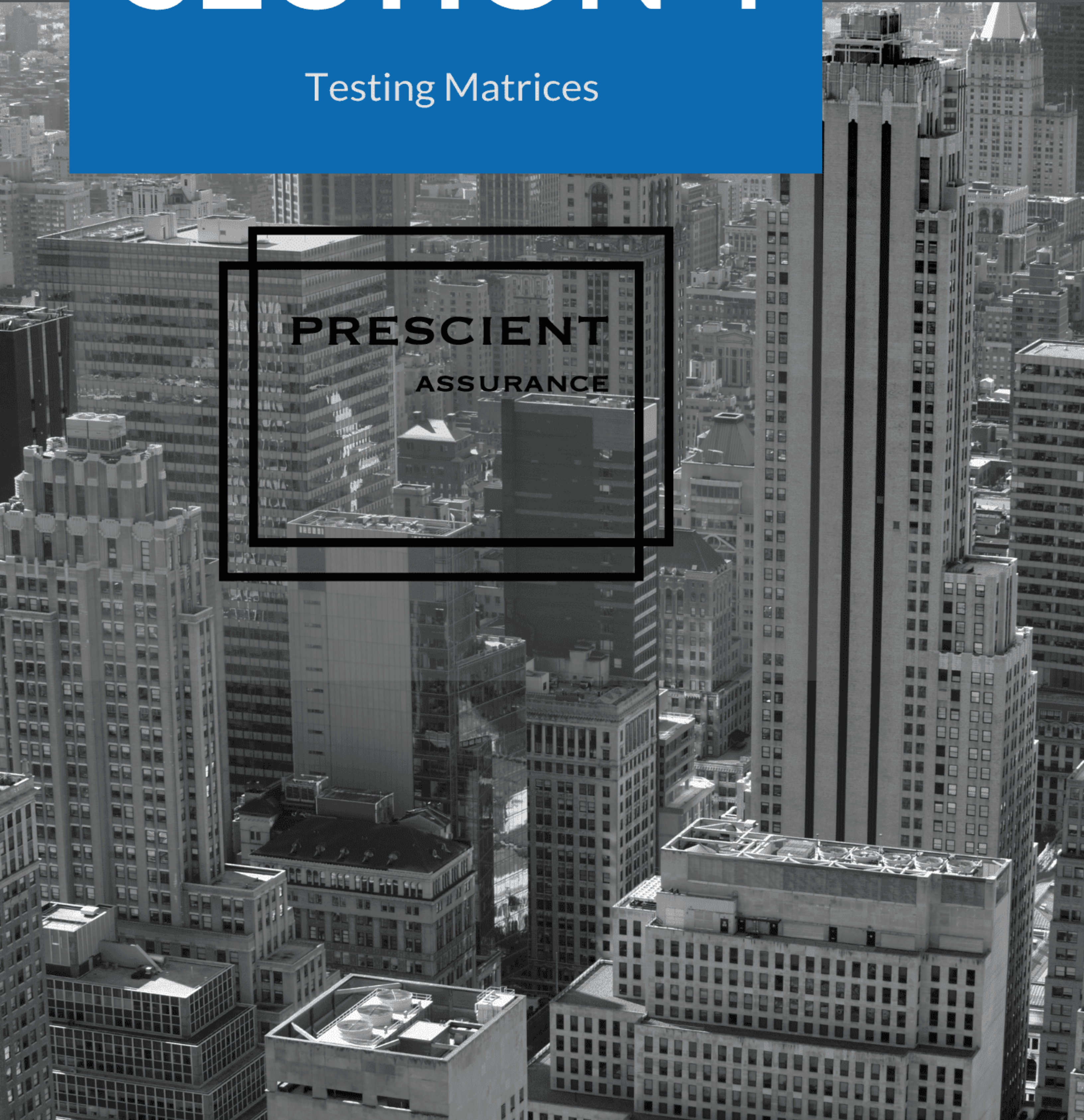
Availability - No HA SLAs are guaranteed as of date, intermittent service un-availability may occur.

DC 9: Disclosure of Significant Changes in Last 1 year

1. Changes to the services provided
    - Launched https://iterative.ai/model-registry
    - Created Billing/Subscription plans (Team plan uses Stripe) - https://iterative.ai/pricing
2. Significant changes to personnel/org structure:
    - Hired Director of Engineering - management changes (CTO managed directly before)
    - Hired 2 Platform Engineers
    - Hired 2 Backend Engineers (1 left, the other will join in Sept) ○ Hiring for the team still ongoing
3. Introduced log collection and rotation
4. Introduced privacy/ security policies and many other SOC2 related changes

SECTION 4

Testing Matrices



PRESCIENT ASSURANCE

Tests of Design and Implementation Effectiveness and Results of Tests

Scope of Testing

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

Prescient Assurance LLC conducted the examination testing as of August 23, 2022.

The tests applied to test the Implementation and Design 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.

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 Implementation and Design Effectiveness of the control activity.

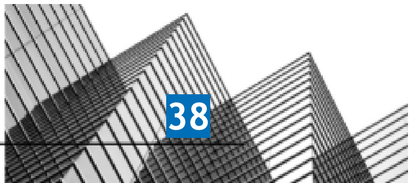
Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

Control Mapping	COSO Principle	Control Description	Test Applied by the Service Auditor	Test Results
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 which states Iterative's expectations against which employee behaviors are evaluated, including the standards for ethical business conduct, corruption, anti-bribery, use of the Internet and social media, conflict of interest, respect, professionalism, and workplace safety, and that violations of the Code shall lead to disciplinary action against the employee, to determine that a Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from Iterative's operations. An information security team has also been established to govern cybersecurity.	Inspected the LinkedIn profiles of Jordan Hollander (Chief of Staff), Dmitry Petrov (Co-Founder & CEO), and Oded Messer (Director of Engineering) to determine that the BoD includes senior management.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inspected the bylaws of Iterative which state that the Board manages the business and affairs of Iterative, directly or by delegating authority to committees and officers as provided by the bylaws, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Moreover, inspected the minutes of a telephonic meeting of the Board held on August 22, 2022, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Internal personnel are evaluated via a formal performance review at least annually.	Inspected the Performance Review Policy which states that performance evaluations are conducted annually with specific dates announced by management and the manager is responsible for the timely and equitable assessment of the performance and contribution of team members, to determine that internal	No exceptions noted.

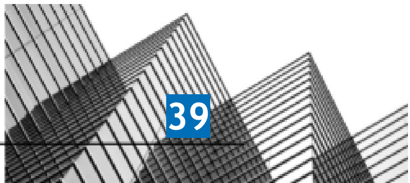
			personnel are evaluated via a formal performance review at least annually.	
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Inspected the Information Security Policy and Code of Conduct which state that any violation of Iterative policies or procedures may result in disciplinary action, up to and including termination of employment, to determine that personnel who violate information security policies are subject to disciplinary action and such disciplinary action is documented in one or more policies.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy which describes the internal control processes, including evaluation and review of the internal controls, approving and implementing changes in internal controls, and third-party communication, to determine that Iterative identifies controls that should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	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 Iterative's operations. An information security team has also been established to govern cybersecurity.	Inspected the LinkedIn profiles of Jordan Hollander (Chief of Staff), Dmitry Petrov (Co-Founder & CEO), and Oded Messer (Director of Engineering) to determine that the BoD includes senior management.	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 bylaws of Iterative which state that the Board manages the business and affairs of Iterative, directly or by delegating authority to committees and officers as provided by the bylaws, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Moreover, inspected the minutes of a telephonic meeting of the Board held on August 22, 2022, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.	No exceptions noted.

CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Internal personnel are evaluated via a formal performance review at least annually.	Inspected the Performance Review Policy which states that performance evaluations are conducted annually with specific dates announced by management and the manager is responsible for the timely and equitable assessment of the performance and contribution of team members, to determine that internal personnel are evaluated via a formal performance review at least annually.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from Iterative's operations. An information security team has also been established to govern cybersecurity.	Inspected the LinkedIn profiles of Jordan Hollander (Chief of Staff), Dmitry Petrov (Co-Founder & CEO), and Oded Messer (Director of Engineering) to determine that the BoD includes senior management.	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 bylaws of Iterative which state that the Board manages the business and affairs of Iterative, directly or by delegating authority to committees and officers as provided by the bylaws, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Moreover, inspected the minutes of a telephonic meeting of the Board held on August 22, 2022, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart to internal personnel.	Inspected Iterative's organizational chart which identifies the positions of the CEO and his direct reports, including the Senior Product Engineer, Solution Engineer, Chief of Staff, Community Manager, Director of Operations, and others, to determine that Iterative maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart to internal personnel.	No exceptions noted.

CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	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 Iterative's Acceptable Use Policy which defines the standards for appropriate and secure use of Iterative's hardware and electronic systems including storage media, communication tools, and internet access, to determine that the Acceptable Use Policy is in place.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	An Information Security Policy establishes the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	Inspected the Information Security Policy, which provides guidelines for ensuring physical, people, and data security, to determine that Iterative has established the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Information security roles and responsibilities are outlined for personnel responsible for the security, availability, and confidentiality of the system.	Inspected the Internal Control Policy, Performance Review Policy, and Security Incident Response Plan which define the responsibilities of the senior management, managers, and Security Response Team, to determine that Iterative's policies outline the roles and responsibilities for personnel with responsibility for the security, availability, and confidentiality of the system.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected the Information Security Policy which states that Iterative requires a vendor security assessment which may include gathering applicable compliance audits (SOC 1, SOC 2, PCI DSS, HITRUST, ISO 27001, etc.) or other security compliance evidence, to determine that vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected the Vendor Management Policy which states that a risk assessment and appropriate due diligence shall be performed for new vendors, to determine that new vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor.	No exceptions noted.

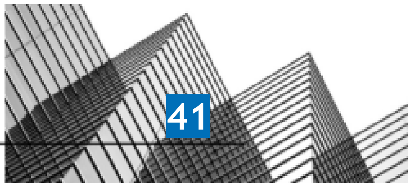


	responsibilities in the pursuit of objectives.			
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control and Termination Policy which defines the requirements for access and removal of access to Iterative data, systems, facilities, and networks, to determine that an Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	An Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls.	Inspected the Encryption and Key Management Policy, which provides guidance on the types of devices and media that need to be encrypted, when encryption must be used, and the minimum standards of the software used for encryption, to determine that Iterative has set out its requirements for generating and rotating, and storing cryptographic keys.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy, which states that production systems handling confidential data are required to have documented baseline configurations, when available, to determine that Iterative's Configuration and Asset Management Policy governs the configurations for new sensitive systems.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected the Change Management Policy, which specifies that change management should be conducted according to a procedure that includes product road mapping, planning and evaluation, building, testing and documenting, reviewing the code, approval and implementation, communication, and post-change review, to determine that the Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain	A Secure Development Policy defines the requirements for secure software and system	Inspected the Secure Development Policy which states that Oded Messer issues procedures for secure information system engineering practices for the development of new systems and for the maintenance of the existing systems, to	No exceptions noted.



	competent individuals in alignment with objectives.	development and maintenance.	determine that Iterative has defined the requirements for secure software and system development and maintenance.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Privacy Policy to both external users and internal personnel. This policy details Iterative's privacy commitments.	Inspected the Privacy & Cookie Policy of Iterative published on "https://iterative.notion.site/Privacy-Cookie-Policy-edbce9b3b3d14f26950b7dca617b2033" which describes the steps taken by Iterative to ensure data privacy, to determine that Iterative publishes its Privacy Policy to both external users and internal personnel and states its privacy commitments.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan which provides guidelines for personnel to detect, report, and respond to incidents through to resolution, to determine that an Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy which defines the basic rules and requirements for network security and ensures the protection of information within and across networks and supporting information processing facilities, to determine that the Network Security Policy identifies the requirements for protecting information and systems within and across networks.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	Inspected the Code of Conduct which states Iterative's expectations against which employee behaviors are evaluated, including the standards for ethical business conduct, corruption, anti-bribery, use of the Internet and social media, conflict of interest, respect, professionalism, and workplace safety, and that violations of the Code shall lead to disciplinary action against the employee, to determine that a Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop,	The board of directors or equivalent entity function includes senior management and external	Inspected the LinkedIn profiles of Jordan Hollander (Chief of Staff), Dmitry Petrov (Co-Founder & CEO), and Oded Messer (Director	No exceptions noted.

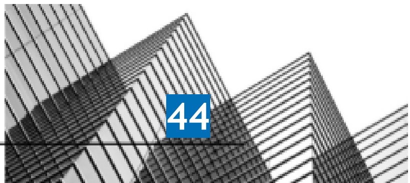
	and retain competent individuals in alignment with objectives.	advisors, who are independent from Iterative's operations. An information security team has also been established to govern cybersecurity.	of Engineering) to determine that the BoD includes senior management.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Internal personnel are evaluated via a formal performance review at least annually.	Inspected the Performance Review Policy which states that performance evaluations are conducted annually with specific dates announced by management and the manager is responsible for the timely and equitable assessment of the performance and contribution of team members, to determine that internal personnel are evaluated via a formal performance review at least annually.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Background checks or their equivalent are performed before or promptly after a new hire's start date, as permitted by local laws.	Inspected the Information Security Policy which states that all Iterative personnel are required to complete a background check by an authorized member of Iterative in accordance with local laws, to determine that background checks are performed on new hires before their start date as permitted by local laws.	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 job descriptions for different positions on Iterative's website (https://iterative.notion.site/Iterative-ai-is-Hiring-852cb978129645e1906e2c9a878a4d22) to determine that Iterative has detailed job descriptions that define the required qualifications, experience, and competency against which applicants are assessed by the hiring managers. Moreover, observed the Employee Confidential Information and Invention Assignment Agreement which includes confidentiality clauses to determine that the new hires are required to sign confidentiality agreements or equivalents upon hire.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in	Internal personnel complete annual training programs for information security to help them understand their obligations and	Inspected the Information Security Policy which states that all personnel are required to undergo training following initial employment and annually thereafter, to determine that internal personnel complete annual training programs for information security to help them understand	No exceptions noted.



	alignment with objectives.	responsibilities related to security.	their obligations and responsibilities related to security, availability, and confidentiality.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	An Acceptable Use Policy defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools and internet access.	Inspected Iterative's Acceptable Use Policy which defines the standards for appropriate and secure use of Iterative's hardware and electronic systems including storage media, communication tools, and internet access, to determine that the Acceptable Use Policy is in place.	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, which provides guidelines for ensuring physical, people, and data security, to determine that Iterative has established 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.	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 which describes the internal control processes, including evaluation and review of the internal controls, approving and implementing changes in internal controls, and third-party communication, to determine that Iterative identifies controls that should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	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 which states that the performance evaluation process provides a means for discussing, planning, and reviewing the performance of each team member, to determine that the Performance Review Policy provides personnel context and transparency into their performance and career development processes.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in	Management is responsible for the design, implementation, and management of the organization's security policies and procedures. The policies and procedures are reviewed by	Inspected the Information Security Policy, Access Control and Termination Policy, and the Business Continuity and Disaster Recovery Plan, which identify Ken Thom as the policy owner, and were last reviewed on Aug 18, 2022, to determine that management is responsible for the design, implementation, and management of the organization's security policies and procedures,	No exceptions noted.

	alignment with objectives.	management at least annually.	and that the policies are periodically reviewed by management at least annually.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Internal personnel review and accept applicable information security policies at least annually.	Inspected the information security policies of Iterative which state that all personnel are required to read, accept, and follow Iterative's policies and plans, to determine that internal personnel review and accept applicable information security policies at least annually.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Information security roles and responsibilities are outlined for personnel responsible for the security, availability, and confidentiality of the system.	Inspected the Internal Control Policy, Performance Review Policy, and Security Incident Response Plan which define the responsibilities of the senior management, managers, and Security Response Team, to determine that Iterative's policies outline the roles and responsibilities for personnel with responsibility for the security, availability, and confidentiality of the system.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, 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 which describes the risk assessment framework and process, to determine that Iterative has a process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Inspected the Vendor Management Policy which states provides a framework for the onboarding, assessment, and management of the vendor relationship lifecycle, including due diligence, risk assessment, contract review, and security controls, to determine that the policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent	Vendor SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	Inspected the Information Security Policy which states that Iterative requires a vendor security assessment which may include gathering applicable compliance audits (SOC 1, SOC 2, PCI DSS, HITRUST, ISO 27001, etc.) or other security compliance evidence, to determine that vendor	No exceptions noted.

	individuals in alignment with objectives.		SOC 2 reports (or equivalent) are collected and reviewed on at least an annual basis.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected the Vendor Management Policy which states that a risk assessment and appropriate due diligence shall be performed for new vendors, to determine that new vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Vulnerability Management and Patch Management Policy outlines the processes to efficiently respond to identified vulnerabilities.	Inspected the Vulnerability Management and Patch Management Policy which states that Iterative schedules third-party security assessments and penetration test and vulnerability scan results to verify vulnerabilities and analyze their impact, to determine that a Vulnerability Management and Patch Management Policy outlines the processes to efficiently respond to identified vulnerabilities.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A Physical Security Policy that details physical security requirements for Iterative facilities is in place.	Inspected the Physical Security Policy which states that Iterative facilities shall be secured via external locked doors and that all facilities shall be monitored via personnel and security cameras to detect potential security threats and respond to alerts, to determine that a Physical Security Policy that details physical security requirements is in place.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from Iterative's operations. An information security team has also been established to govern cybersecurity.	Inspected the LinkedIn profiles of Jordan Hollander (Chief of Staff), Dmitry Petrov (Co-Founder & CEO), and Oded Messer (Director of Engineering) to determine that the BoD includes senior management.	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	Inspected the bylaws of Iterative which state that the Board manages the business and affairs of Iterative, directly or by delegating authority to committees and officers as provided by the bylaws, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk	No exceptions noted.



		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.	management activities, and other internal/external matters. Moreover, inspected the minutes of a telephonic meeting of the Board held on August 22, 2022, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.	
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Internal personnel are evaluated via a formal performance review at least annually.	Inspected the Performance Review Policy which states that performance evaluations are conducted annually with specific dates announced by management and the manager is responsible for the timely and equitable assessment of the performance and contribution of team members, to determine that internal personnel are evaluated via a formal performance review at least annually.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy, which states that Iterative manages and maintains its internal controls using the Secureframe platform, to determine that a continuous monitoring solution monitors the 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.	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 Iterative's organizational chart which identifies the positions of the CEO and his direct reports, including the Senior Product Engineer, Solution Engineer, Chief of Staff, Community Manager, Director of Operations, and others, to determine that Iterative maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart to internal personnel.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill their responsibilities. New hires sign confidentiality agreements or equivalents upon hire.	Inspected the job descriptions for different positions on Iterative's website (https://iterative.notion.site/Iterative-ai-is-Hiring-852cb978129645e1906e2c9a878a4d22) to determine that Iterative has detailed job descriptions that define the required qualifications, experience, and competency against which applicants are assessed by the hiring managers. Moreover, observed the Employee Confidential Information and Invention Assignment Agreement	No exceptions noted.

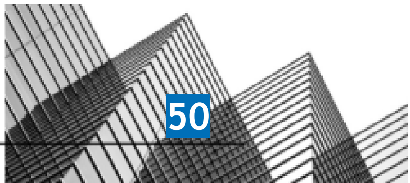
			which includes confidentiality clauses to determine that the new hires are required to sign confidentiality agreements or equivalents upon hire.	
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Personnel who violate information security policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.	Inspected the Information Security Policy and Code of Conduct which state that any violation of Iterative policies or procedures may result in disciplinary action, up to and including termination of employment, to determine that personnel who violate information security policies are subject to disciplinary action and such disciplinary action is documented in one or more policies.	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 which describes the internal control processes, including evaluation and review of the internal controls, approving and implementing changes in internal controls, and third-party communication, to determine that Iterative identifies controls that 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.	A Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Inspected the Performance Review Policy which states that the performance evaluation process provides a means for discussing, planning, and reviewing the performance of each team member, to determine that the Performance Review Policy provides personnel context and transparency into their performance and career development processes.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy which states that the changes must be tested in an Iterative staging environment before the production release, to determine that software changes are tested before being deployed into production.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy, which states that Iterative manages and maintains its internal controls using the Secureframe platform, to determine that a continuous monitoring solution monitors the 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.	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment and Treatment Policy, which states that Iterative follows a risk assessment framework and process for identifying, analyzing, scoring, and mitigating risks, and that risk assessments must be conducted at least annually or whenever there are significant changes to Iterative or its systems, to determine that formal risk assessments are performed.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected the Vulnerability and Patch Management Policy which states that Iterative periodically tests the security posture of its applications and systems through third-party testing and vulnerability scanning, to determine that vulnerability scanning is performed on production infrastructure systems regularly.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	A 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Inspected the Vulnerability and Patch Management Policy which states that Iterative schedules third-party penetration tests at least annually to determine that a third party is engaged to conduct a network and application penetration test of the production environment at least annually.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected the Configuration and Asset Management Policy which states that production systems handling confidential data must have documented baseline configurations, when available, to determine that baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	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.	Development, staging, and production environments are segregated.	Inspected the Information Security Policy which states that Iterative maintains requirements and controls for the separation of the development and production environments, to determine that the production, development, and staging environments are segregated.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives	Production data is not used in the development and testing environments,	Inspected the Secure Development Policy which states that Iterative requires confidential and restricted data not to be used as test data, except where required for customer debugging,	No exceptions noted.

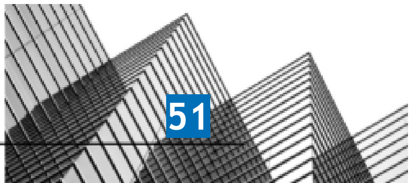
	and responsibilities for internal control, necessary to support the functioning of internal control.	unless required for debugging customer issues.	to determine that production data is not used in the development and testing environments.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy, which states that production systems handling confidential data are required to have documented baseline configurations, when available, to determine that Iterative's Configuration and Asset Management Policy governs the configurations for new sensitive systems.	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.	Security commitments and expectations are communicated to both internal personnel and external users via Iterative's website.	Inspected the Privacy & Cookie Policy of Iterative published on "https://iterative.notion.site/Privacy-Cookie-Policy-edbce9b3b3d14f26950b7dca617b2033" which describes the data security measures taken by Iterative, to determine that security commitments and expectations are communicated to external users via Iterative's Privacy & Cookie Policy.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Terms of Service or the equivalent are published or shared to external users.	Inspected the Privacy & Cookie Policy of Iterative published on "https://iterative.notion.site/Privacy-Cookie-Policy-edbce9b3b3d14f26950b7dca617b2033", which states the data use and disclosure policies, to determine that Terms of Service or the equivalent are published or shared to external users.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	A Privacy Policy to both external users and internal personnel. This policy details Iterative's privacy commitments.	Inspected the Privacy & Cookie Policy of Iterative published on "https://iterative.notion.site/Privacy-Cookie-Policy-edbce9b3b3d14f26950b7dca617b2033" which describes the steps taken by Iterative to ensure data privacy, to determine that Iterative publishes its Privacy Policy to both external users and internal personnel and states its privacy commitments.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control,	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed	Inspected the Security Incident Response Plan which provides guidelines for personnel to detect, report, and respond to incidents through to resolution, to determine that an Incident Response Plan outlines the process of identifying, prioritizing, communicating,	No exceptions noted.

	necessary to support the functioning of internal control.	incidents through to resolution.	assigning, and tracking confirmed incidents through to resolution.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inspected the Internal Control Policy which states that Iterative requires all issues that impact internal control to be tracked and monitored until the resolution is implemented, to determine that identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	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 which defines the basic rules and requirements for network security and ensures the protection of information within and across networks and supporting information processing facilities, to determine that the Network Security Policy identifies the requirements for protecting information and systems within and across networks.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	A Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	Inspected the Code of Conduct which states Iterative's expectations against which employee behaviors are evaluated, including the standards for ethical business conduct, corruption, anti-bribery, use of the Internet and social media, conflict of interest, respect, professionalism, and workplace safety, and that violations of the Code shall lead to disciplinary action against the employee, to determine that a Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from Iterative's operations. An information security team has also been established to govern cybersecurity.	Inspected the LinkedIn profiles of Jordan Hollander (Chief of Staff), Dmitry Petrov (Co-Founder & CEO), and Oded Messer (Director of Engineering) to determine that the BoD includes senior management.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives	Internal personnel complete annual training programs for information security to help them	Inspected the Information Security Policy which states that all personnel are required to undergo training following initial employment and annually thereafter, to determine that internal	No exceptions noted.

	and responsibilities for internal control, necessary to support the functioning of internal control.	understand their obligations and responsibilities related to security.	personnel complete annual training programs for information security to help them understand their obligations and responsibilities related to security, availability, and confidentiality.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	An Acceptable Use Policy defines standards for appropriate and secure use of company hardware and electronic systems including storage media, communication tools and internet access.	Inspected Iterative's Acceptable Use Policy which defines the standards for appropriate and secure use of Iterative's hardware and electronic systems including storage media, communication tools, and internet access, to determine that the Acceptable Use Policy is in place.	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 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, which provides guidelines for ensuring physical, people, and data security, to determine that Iterative has established the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy which describes the internal control processes, including evaluation and review of the internal controls, approving and implementing changes in internal controls, and third-party communication, to determine that Iterative identifies controls that should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Management is responsible for the design, implementation, and management of the organization's security policies and procedures. The policies and procedures are reviewed by management at least annually.	Inspected the Information Security Policy, Access Control and Termination Policy, and the Business Continuity and Disaster Recovery Plan, which identify Ken Thom as the policy owner, and were last reviewed on Aug 18, 2022, to determine that management is responsible for the design, implementation, and management of the organization's security policies and procedures, and that the policies are periodically reviewed by management at least annually.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives	Internal personnel review and accept applicable information security policies at least annually.	Inspected the information security policies of Iterative which state that all personnel are required to read, accept, and follow Iterative's policies and plans, to determine that internal	No exceptions noted.



	and responsibilities for internal control, necessary to support the functioning of internal control.		personnel review and accept applicable information security policies at least annually.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Information security roles and responsibilities are outlined for personnel responsible for the security, availability, and confidentiality of the system.	Inspected the Internal Control Policy, Performance Review Policy, and Security Incident Response Plan which define the responsibilities of the senior management, managers, and Security Response Team, to determine that Iterative's policies outline the roles and responsibilities for personnel with responsibility for the security, availability, and confidentiality of the system.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected the Configuration and Asset Management Policy which states that production systems handling confidential data must have documented baseline configurations, when available, to determine that baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Development, staging, and production environments are segregated.	Inspected the Information Security Policy which states that Iterative maintains requirements and controls for the separation of the development and production environments, to determine that the production, development, and staging environments are segregated.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Production data is not used in the development and testing environments, unless required for debugging customer issues.	Inspected the Secure Development Policy which states that Iterative requires confidential and restricted data not to be used as test data, except where required for customer debugging, to determine that production data is not used in the development and testing environments.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy, which states that production systems handling confidential data are required to have documented baseline configurations, when available, to determine that Iterative's Configuration and Asset Management Policy governs the configurations for new sensitive systems.	No exceptions noted.
CC2.3	The entity communicates with external parties	Security commitments and expectations are communicated to both	Inspected the Privacy & Cookie Policy of Iterative published on "https://iterative.notion.site/Privacy-Cookie-Poli	No exceptions noted.

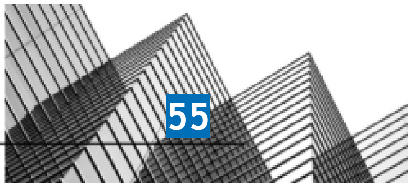


	regarding matters affecting the functioning of internal control.	internal personnel and external users via Iterative's website.	cy-edbce9b3b3d14f26950b7dca617b2033" which describes the data security measures taken by Iterative, to determine that security commitments and expectations are communicated to external users via Iterative's Privacy & Cookie Policy.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Terms of Service or the equivalent are published or shared to external users.	Inspected the Privacy & Cookie Policy of Iterative published on "https://iterative.notion.site/Privacy-Cookie-Policy-edbce9b3b3d14f26950b7dca617b2033", which states the data use and disclosure policies, to determine that Terms of Service or the equivalent are published or shared to external users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	A confidential reporting channel is made available to internal personnel and external parties to report security and other identified concerns.	Inspected the Security Incident Response Plan, which provides an email address (security@iterative.ai) to determine that a confidential reporting channel is made available to 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 to both external users and internal personnel. This policy details Iterative's privacy commitments.	Inspected the Privacy & Cookie Policy of Iterative published on "https://iterative.notion.site/Privacy-Cookie-Policy-edbce9b3b3d14f26950b7dca617b2033" which describes the steps taken by Iterative to ensure data privacy, to determine that Iterative publishes its Privacy Policy to both external users and internal personnel and states its privacy commitments.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inspected the Internal Control Policy which states that Iterative requires all issues that impact internal control to be tracked and monitored until the resolution is implemented, to determine that identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	A Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy which defines the basic rules and requirements for network security and ensures the protection of information within and across networks and supporting information processing facilities, to determine that the Network Security Policy identifies the requirements for protecting information and systems within and across networks.	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 Management Policy which states that a risk assessment and appropriate due diligence shall be performed for new vendors, to determine that new vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inspected the bylaws of Iterative which state that the Board manages the business and affairs of Iterative, directly or by delegating authority to committees and officers as provided by the bylaws, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Moreover, inspected the minutes of a telephonic meeting of the Board held on August 22, 2022, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.	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 which describes the risk assessment framework and process, to determine that Iterative has a process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment and Treatment Policy, which states that Iterative follows a risk assessment framework and process for identifying, analyzing, scoring, and mitigating risks, and that risk assessments must be conducted at least annually or whenever there are significant changes to Iterative or its systems, to determine that formal risk assessments are performed.	No exceptions noted.

CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	A list of system assets, components, and respective owners are maintained and reviewed at least annually.	Inspected the Configuration and Asset Management Policy which states that Iterative inventories and tracks all assets that are used to process, store, transmit, or otherwise impact the confidentiality, integrity, or availability of sensitive information, and that Ken Thom or a designee will be held accountable for the accuracy of the inventory and must audit the asset list at least annually, to determine that Iterative maintains a list of Iterative's system components and owners and reviews it at least annually.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	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 bylaws of Iterative which state that the Board manages the business and affairs of Iterative, directly or by delegating authority to committees and officers as provided by the bylaws, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Moreover, inspected the minutes of a telephonic meeting of the Board held on August 22, 2022, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.	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 which describes the risk assessment framework and process, to determine that Iterative has a process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners.	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	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud,	Inspected the Risk Assessment and Treatment Policy, which states that Iterative follows a risk assessment framework and process for identifying, analyzing, scoring, and mitigating risks, and that risk assessments must be conducted at least annually or whenever there are significant changes to Iterative or its	No exceptions noted.

	risks should be managed.	and an analysis of risks associated with those threats.	systems, to determine that formal risk assessments are performed.	
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 of Iterative maintained on Secureframe, identifying 4 risks with an assigned risk owner, 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.	A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Inspected the Vendor Management Policy which states provides a framework for the onboarding, assessment, and management of the vendor relationship lifecycle, including due diligence, risk assessment, contract review, and security controls, to determine that the policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	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 Management Policy which states that a risk assessment and appropriate due diligence shall be performed for new vendors, to determine that new vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Inspected the Risk Assessment and Treatment Policy which describes the risk assessment framework and process, to determine that Iterative has a process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to	Inspected the Risk Assessment and Treatment Policy, which states that Iterative follows a risk assessment framework and process for identifying, analyzing, scoring, and mitigating risks, and that risk assessments must be	No exceptions noted.



	achievement of objectives.	security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	conducted at least annually or whenever there are significant changes to Iterative or its systems, to determine that formal risk assessments are performed.	
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy which describes the internal control processes, including evaluation and review of the internal controls, approving and implementing changes in internal controls, and third-party communication, to determine that Iterative identifies controls that should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Inspected the Risk Assessment and Treatment Policy which describes the risk assessment framework and process, to determine that Iterative has a process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners.	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 Risk Assessment and Treatment Policy, which states that Iterative follows a risk assessment framework and process for identifying, analyzing, scoring, and mitigating risks, and that risk assessments must be conducted at least annually or whenever there are significant changes to Iterative or its systems, to determine that formal risk assessments are performed.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	A Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	Inspected the Vendor Management Policy which states provides a framework for the onboarding, assessment, and management of the vendor relationship lifecycle, including due diligence, risk assessment, contract review, and security controls, to determine that the policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	No exceptions noted.

CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected the Vendor Management Policy which states that a risk assessment and appropriate due diligence shall be performed for new vendors, to determine that new vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor.	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.	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy which states that the changes must be tested in an Iterative staging environment before the production release, to determine that software changes are tested before being deployed into production.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy, which states that Iterative manages and maintains its internal controls using the Secureframe platform, to determine that a continuous monitoring solution monitors the 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.	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected the Vulnerability and Patch Management Policy which states that Iterative periodically tests the security posture of its applications and systems through third-party testing and vulnerability scanning, to determine that vulnerability scanning is performed on production infrastructure systems regularly.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	A 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Inspected the Vulnerability and Patch Management Policy which states that Iterative schedules third-party penetration tests at least annually to determine that a third party is engaged to conduct a network and application penetration test of the production environment at least annually.	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.	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy which states that the changes must be tested in an Iterative staging environment before the production release, to determine that software changes are tested before being deployed into production.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	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 bylaws of Iterative which state that the Board manages the business and affairs of Iterative, directly or by delegating authority to committees and officers as provided by the bylaws, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Moreover, inspected the minutes of a telephonic meeting of the Board held on August 22, 2022, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy, which states that Iterative manages and maintains its internal controls using the Secureframe platform, to determine that a continuous monitoring solution monitors the internal controls used in the achievement of service commitments and system requirements.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are	Inspected the Vulnerability and Patch Management Policy which states that Iterative periodically tests the security posture of its applications and systems through third-party testing and vulnerability scanning, to determine	No exceptions noted.

	those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	remediated on a timely basis.	that vulnerability scanning is performed on production infrastructure systems regularly.	
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	A 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Inspected the Vulnerability and Patch Management Policy which states that Iterative schedules third-party penetration tests at least annually to determine that a third party is engaged to conduct a network and application penetration test of the production environment at least annually.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	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 bylaws of Iterative which state that the Board manages the business and affairs of Iterative, directly or by delegating authority to committees and officers as provided by the bylaws, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Moreover, inspected the minutes of a telephonic meeting of the Board held on August 22, 2022, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy, which states that Iterative manages and maintains its internal controls using the Secureframe platform, to determine that a continuous monitoring solution monitors the internal controls used in the achievement of service commitments and system requirements.	No exceptions noted.

CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	An Internal Control Policy identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	Inspected the Internal Control Policy which describes the internal control processes, including evaluation and review of the internal controls, approving and implementing changes in internal controls, and third-party communication, to determine that Iterative identifies controls that should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Formal risk assessments are performed, which includes the identification of relevant internal and external threats related to security, availability, confidentiality, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment and Treatment Policy, which states that Iterative follows a risk assessment framework and process for identifying, analyzing, scoring, and mitigating risks, and that risk assessments must be conducted at least annually or whenever there are significant changes to Iterative or its systems, to determine that formal risk assessments are performed.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	A risk register is maintained, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.	Inspected the risk register of Iterative maintained on Secureframe, identifying 4 risks with an assigned risk owner, 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.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	A list of system assets, components, and respective owners are maintained and reviewed at least annually.	Inspected the Configuration and Asset Management Policy which states that Iterative inventories and tracks all assets that are used to process, store, transmit, or otherwise impact the confidentiality, integrity, or availability of sensitive information, and that Ken Thom or a designee will be held accountable for the accuracy of the inventory and must audit the asset list at least annually, to determine that Iterative maintains a list of Iterative's system components and owners and reviews it at least annually.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected the Secure Development Policy which states that Oded Messer issues procedures for secure information system engineering practices for the development of new systems and for the maintenance of the existing systems, to determine that Iterative has defined the	No exceptions noted.

	achievement of objectives.		requirements for secure software and system development and maintenance.	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inspected the bylaws of Iterative which state that the Board manages the business and affairs of Iterative, directly or by delegating authority to committees and officers as provided by the bylaws, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Moreover, inspected the minutes of a telephonic meeting of the Board held on August 22, 2022, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy, which states that Iterative manages and maintains its internal controls using the Secureframe platform, to determine that a continuous monitoring solution monitors the 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.	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, which provides guidelines for ensuring physical, people, and data security, to determine that Iterative has established the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and data.	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 which describes the internal control processes, including evaluation and review of the internal controls, approving and implementing changes in internal controls, and third-party communication, to determine that Iterative identifies controls that 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	Information security roles and responsibilities are outlined for personnel	Inspected the Internal Control Policy, Performance Review Policy, and Security Incident Response Plan which define the responsibilities	No exceptions noted.

	activities over technology to support the achievement of objectives.	responsible for the security, availability, and confidentiality of the system.	of the senior management, managers, and Security Response Team, to determine that Iterative's policies outline the roles and responsibilities for personnel with responsibility for the security, availability, and confidentiality of the system.	
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 which defines the requirements for access and removal of access to Iterative data, systems, facilities, and networks, to determine that an Access Control and Termination Policy governs 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.	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, which provides guidance on the types of devices and media that need to be encrypted, when encryption must be used, and the minimum standards of the software used for encryption, to determine that Iterative has set out its requirements for generating and rotating, and storing cryptographic keys.	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, which states that production systems handling confidential data are required to have documented baseline configurations, when available, to determine that Iterative's Configuration and Asset Management Policy governs 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, which specifies that change management should be conducted according to a procedure that includes product road mapping, planning and evaluation, building, testing and documenting, reviewing the code, approval and implementation, communication, and post-change review, to determine that the Change Management Policy 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	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected the Secure Development Policy which states that Oded Messer issues procedures for secure information system engineering practices for the development of new systems and for the maintenance of the existing systems, to determine that Iterative has defined the	No exceptions noted.

	procedures that put policies into action.		requirements for secure software and system development and maintenance.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	A Privacy Policy to both external users and internal personnel. This policy details Iterative's privacy commitments.	Inspected the Privacy & Cookie Policy of Iterative published on "https://iterative.notion.site/Privacy-Cookie-Policy-edbce9b3b3d14f26950b7dca617b2033" which describes the steps taken by Iterative to ensure data privacy, to determine that Iterative publishes its Privacy Policy to both external users and internal personnel and states its privacy commitments.	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 Response Plan which provides guidelines for personnel to detect, report, and respond to incidents through to resolution, to determine that an Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through 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 Network Security Policy identifies the requirements for protecting information and systems within and across networks.	Inspected the Network Security Policy which defines the basic rules and requirements for network security and ensures the protection of information within and across networks and supporting information processing facilities, to determine that the Network Security Policy identifies the requirements for protecting information and systems within and across 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 Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	Inspected the Code of Conduct which states Iterative's expectations against which employee behaviors are evaluated, including the standards for ethical business conduct, corruption, anti-bribery, use of the Internet and social media, conflict of interest, respect, professionalism, and workplace safety, and that violations of the Code shall lead to disciplinary action against the employee, to determine that a Code of Conduct outlines ethical expectations, behavior standards, and ramifications of noncompliance.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy, which states that Iterative manages and maintains its internal controls using the Secureframe platform, to determine that a continuous monitoring solution monitors the 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.	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 Iterative's Acceptable Use Policy which defines the standards for appropriate and secure use of Iterative's hardware and electronic systems including storage media, communication tools, and internet access, to determine that the Acceptable Use Policy 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.	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, which provides guidelines for ensuring physical, people, and data security, to determine that Iterative has established the security requirements for maintaining the security, confidentiality, integrity, and availability of applications, systems, infrastructure, and 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.	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 which describes the internal control processes, including evaluation and review of the internal controls, approving and implementing changes in internal controls, and third-party communication, to determine that Iterative identifies controls that 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 Performance Review Policy provides personnel context and transparency into their performance and career development processes.	Inspected the Performance Review Policy which states that the performance evaluation process provides a means for discussing, planning, and reviewing the performance of each team member, to determine that the Performance Review Policy provides personnel context and transparency into their performance and career development processes.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Management is responsible for the design, implementation, and management of the organization's security policies and procedures. The policies and procedures are reviewed by management at least annually.	Inspected the Information Security Policy, Access Control and Termination Policy, and the Business Continuity and Disaster Recovery Plan, which identify Ken Thom as the policy owner, and were last reviewed on Aug 18, 2022, to determine that management is responsible for the design, implementation, and management of the organization's security policies and procedures, and that the policies are periodically reviewed by management at least annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that	Internal personnel review and accept applicable	Inspected the information security policies of Iterative which state that all personnel are required to read, accept, and follow Iterative's	No exceptions noted.

	establish what is expected and in procedures that put policies into action.	information security policies at least annually.	policies and plans, to determine that internal personnel review and accept applicable information security policies at least annually.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Information security roles and responsibilities are outlined for personnel responsible for the security, availability, and confidentiality of the system.	Inspected the Internal Control Policy, Performance Review Policy, and Security Incident Response Plan which define the responsibilities of the senior management, managers, and Security Response Team, to determine that Iterative's policies outline the roles and responsibilities for personnel with responsibility for the security, availability, and confidentiality of the system.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	A Risk Assessment and Treatment Policy governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners. Risk tolerance and strategies are also defined in the policy.	Inspected the Risk Assessment and Treatment Policy which describes the risk assessment framework and process, to determine that Iterative has a process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners.	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 which states provides a framework for the onboarding, assessment, and management of the vendor relationship lifecycle, including due diligence, risk assessment, contract review, and security controls, to determine that the policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	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 which states that Iterative schedules third-party security assessments and penetration test and vulnerability scan results to verify vulnerabilities and analyze their impact, to determine that a Vulnerability Management and Patch Management Policy 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	A Physical Security Policy that details physical security requirements for Iterative facilities is in place.	Inspected the Physical Security Policy which states that Iterative facilities shall be secured via external locked doors and that all facilities shall be monitored via personnel and security cameras to detect potential security threats and	No exceptions noted.

	procedures that put policies into action.		respond to alerts, to determine that a Physical Security Policy that details physical security requirements is in place.	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	A list of system assets, components, and respective owners are maintained and reviewed at least annually.	Inspected the Configuration and Asset Management Policy which states that Iterative inventories and tracks all assets that are used to process, store, transmit, or otherwise impact the confidentiality, integrity, or availability of sensitive information, and that Ken Thom or a designee will be held accountable for the accuracy of the inventory and must audit the asset list at least annually, to determine that Iterative maintains a list of Iterative's system components and owners and reviews it at least annually.	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 the Access Control and Termination Policy which states that Iterative provides users of Iterative systems and applications with unique credentials (IDs, keys, etc.) to determine that users are assigned unique IDs to access sensitive 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.	Personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	Inspected the Access Control and Termination Policy which states that complex passwords are required for all users and multi-factor authentication is required for access to company email, version control tools, and cloud infrastructure, to determine that personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information. Moreover, inspected the Data Retention and Disposal Policy, to determine that Iterative allows only a limited number of employees to have access to customer data.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control and Termination Policy which defines the requirements for access and removal of access to Iterative data, systems, facilities, and networks, to determine that an Access Control and Termination Policy governs	No exceptions noted.

	protected information assets to protect them from security events to meet the entity's objectives.		authentication and access to applicable systems, data, and networks.	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	Inspected the Access Control and Termination Policy which states that Iterative adheres to the principle of least privilege, specifying that users of Iterative systems should be given minimum access to data and systems based on job function, business requirements, or need-to-know for that specific user and that users of Iterative systems and applications will be provided with unique credentials, to determine that non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy which states that administrative access to production servers and databases is restricted based on the principle of least privilege for personnel who have a job function and business need for such access, to determine that administrative access to production infrastructure is restricted based on the principle of least privilege.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy which states that administrative access to production servers and databases is restricted based on the principle of least privilege for personnel who have a job function and business need for such access, to determine that administrative access to production infrastructure is restricted based on the principle of least privilege.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and	Upon termination or when internal personnel no longer require access, system access is removed, as applicable.	Inspected the Offboarding Procedures within the Access Control and Termination Policy which state that Iterative requires an offboarding email or ticket to be sent to IT/Engineering after an employee's resignation or termination and that	No exceptions noted.

	architectures over protected information assets to protect them from security events to meet the entity's objectives.		IT/Engineering is required to revoke the employee's access to Iterative systems, applications, and physical access points (as applicable) within 24 hours of the last day with Iterative, or sooner, if necessary, to determine that upon termination or when internal personnel no longer require access, infrastructure, and application access is removed.	
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 Configuration and Asset Management Policy which states that Iterative requires hard disks to be encrypted at rest by using FileVault for MacOS, LUKS for Linux, and Bitlocker for Windows operating systems, to determine that service data is encrypted at rest. Moreover, inspected the Encryption and Key Management Policy which states that Iterative requires data encryption at rest and shall only include strong encryption methods, to determine that Iterative is required to implement encryption-at-rest for service data.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	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, which provides guidance on the types of devices and media that need to be encrypted, when encryption must be used, and the minimum standards of the software used for encryption, to determine that Iterative has set out its requirements for generating and rotating, and storing cryptographic keys.	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.	Development, staging, and production environments are segregated.	Inspected the Information Security Policy which states that Iterative maintains requirements and controls for the separation of the development and production environments, to determine that the production, development, and staging environments are segregated.	No exceptions noted.

CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected the Secure Development Policy which states that Oded Messer issues procedures for secure information system engineering practices for the development of new systems and for the maintenance of the existing systems, to determine that Iterative has defined the requirements for secure software and system development and maintenance.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Descriptions of Iterative's services and systems are available to both internal personnel and external users.	Inspected the details of Iterative's solutions and products published on "https://iterative.ai/model-registry" and "https://iterative.ai/experiment-tracking" to determine that descriptions of Iterative's services are available to both internal personnel and external users.	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 Acceptable Use Policy which states that Mobile Device Management (MDM) is implemented to manage and enforce mobile device configuration and security policies, including password policies, encryption, malware protection, and security updates, to determine that 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	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected the Network Security Policy which states that Iterative utilizes threat monitoring solutions to detect and alert the management about network-based threats, to determine that security tools are implemented to provide monitoring of network traffic to the production environment.	No exceptions noted.

	meet the entity's objectives.			
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	Inspected the Network Security Policy which states that Iterative requires networking ports and protocols to be restricted based on the least functionality principle, to determine that configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	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.	Personnel are assigned unique IDs to access sensitive systems, networks, and information.	Inspected the Access Control and Termination Policy which states that Iterative provides users of Iterative systems and applications with unique credentials (IDs, keys, etc.) to determine that users are assigned unique IDs to access sensitive information.	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	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control and Termination Policy which defines the requirements for access and removal of access to Iterative data, systems, facilities, and networks, to determine that an Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	No exceptions noted.

	user access is no longer authorized.			
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.	Non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	Inspected the Access Control and Termination Policy which states that Iterative adheres to the principle of least privilege, specifying that users of Iterative systems should be given minimum access to data and systems based on job function, business requirements, or need-to-know for that specific user and that users of Iterative systems and applications will be provided with unique credentials, to determine that non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy which states that administrative access to production servers and databases is restricted based on the principle of least privilege for personnel who have a job function and business need for such access, 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	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy which states that administrative access to production servers and databases is restricted based on the principle of least privilege for personnel who have a job function and business need for such access, to determine that administrative access to production infrastructure is restricted based on the principle of least privilege.	No exceptions noted.

	is administered by the entity, user system credentials are removed when user access is no longer authorized.			
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 Offboarding Procedures within the Access Control and Termination Policy which state that Iterative requires an offboarding email or ticket to be sent to IT/Engineering after an employee's resignation or termination and that IT/Engineering is required to revoke the employee's access to Iterative systems, applications, and physical access points (as applicable) within 24 hours of the last day with Iterative, or sooner, if necessary, to determine that upon termination or when internal personnel no longer require access, infrastructure, and application access is removed.	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 Access Control and Termination Policy which states that Iterative requires a team manager to review, audit, and document user accounts and associated privileges of at least high-risk and critical vendors at least quarterly, to determine that system owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets	Personnel are assigned unique IDs to access sensitive systems, networks, and information.	Inspected the Access Control and Termination Policy which states that Iterative provides users of Iterative systems and applications with unique credentials (IDs, keys, etc.) to determine that users are assigned unique IDs to access sensitive information.	No exceptions noted.

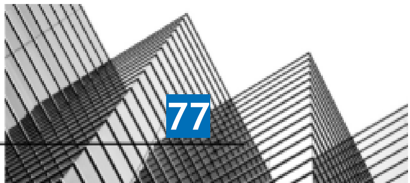
	based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control and Termination Policy which defines the requirements for access and removal of access to Iterative data, systems, facilities, and networks, to determine that an Access Control and Termination Policy governs 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 Access Control and Termination Policy which states that Iterative adheres to the principle of least privilege, specifying that users of Iterative systems should be given minimum access to data and systems based on job function, business requirements, or need-to-know for that specific user and that users of Iterative systems and applications will be provided with unique credentials, to determine that non-console access to production infrastructure is restricted to users with a unique SSH key or access key.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to	Administrative access to production infrastructure is	Inspected the Access Control and Termination Policy which states that administrative access to production servers and databases is restricted	No exceptions noted.

	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.	restricted based on the principle of least privilege.	based on the principle of least privilege for personnel who have a job function and business need for such access, to determine that administrative access to production infrastructure is restricted based on the principle of least privilege.	
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy which states that administrative access to production servers and databases is restricted based on the principle of least privilege for personnel who have a job function and business need for such access, to determine that administrative access to production infrastructure is restricted 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 concepts of least privilege and segregation of	Upon termination or when internal personnel no longer require access, system access is removed, as applicable.	Inspected the Offboarding Procedures within the Access Control and Termination Policy which state that Iterative requires an offboarding email or ticket to be sent to IT/Engineering after an employee's resignation or termination and that IT/Engineering is required to revoke the employee's access to Iterative systems, applications, and physical access points (as applicable) within 24 hours of the last day with Iterative, or sooner, if necessary, to determine that upon termination or when internal personnel no longer require access, infrastructure, and application access is removed.	No exceptions noted.

	duties, to meet the entity's objectives.			
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	System owners conduct scheduled user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	Inspected the Access Control and Termination Policy which states that Iterative requires a team manager to review, audit, and document user accounts and associated privileges of at least high-risk and critical vendors at least quarterly, to determine that system owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.	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.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control and Termination Policy which defines the requirements for access and removal of access to Iterative data, systems, facilities, and networks, to determine that an Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy which states that administrative access to production servers and databases is restricted based on the principle of least privilege for personnel who have a job function and business need for such access, to determine that administrative access to production infrastructure is restricted based on the principle of least privilege.	No exceptions noted.

CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy which states that administrative access to production servers and databases is restricted based on the principle of least privilege for personnel who have a job function and business need for such access, to determine that administrative access to production infrastructure is restricted based on the principle of least privilege.	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.	Upon termination or when internal personnel no longer require access, system access is removed, as applicable.	Inspected the Offboarding Procedures within the Access Control and Termination Policy which state that Iterative requires an offboarding email or ticket to be sent to IT/Engineering after an employee's resignation or termination and that IT/Engineering is required to revoke the employee's access to Iterative systems, applications, and physical access points (as applicable) within 24 hours of the last day with Iterative, or sooner, if necessary, to determine that upon termination or when internal personnel no longer require access, infrastructure, and application access is removed.	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 Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy, which states that production systems handling confidential data are required to have documented baseline configurations, when available, to determine that Iterative's Configuration and Asset Management Policy governs the configurations for new sensitive systems.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets	A Physical Security Policy that details physical security requirements for Iterative facilities is in place.	Inspected the Physical Security Policy which states that Iterative facilities shall be secured via external locked doors and that all facilities shall be monitored via personnel and security cameras to detect potential security threats and	No exceptions noted.

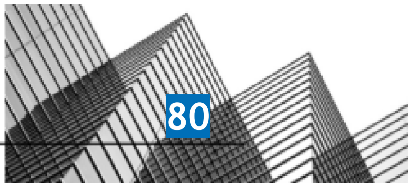
	(for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		respond to alerts, to determine that a Physical Security Policy that details physical security requirements is in place.	
CC6.4	The entity restricts physical 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 Iterative facilities is in place.	Inspected the Physical Security Policy which states that Iterative facilities shall be secured via external locked doors and that all facilities shall be monitored via personnel and security cameras to detect potential security threats and respond to alerts, to determine that a Physical Security Policy that details physical security requirements is in place.	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.	Production facilities require all visitors to formally sign-in, unless preauthorization for the visitor exists.	Inspected the Physical Security Policy which states that all visitors must sign in with security prior to being allowed in the internal office area, to determine that production facilities require all visitors to formally sign in unless preauthorization for the visitor exists.	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)	Processes are in place to create, modify or remove physical access to facilities such as data centers, office spaces, and work areas based on the needs of such individuals.	Inspected the Physical Security Policy which states that Iterative utilizes access cards or keys to unlock external doors throughout all business hours, to determine that processes are in place to create, modify, or remove physical access to facilities such as data centers, office spaces, and work areas based on the needs of such individual.	No exceptions noted.



	to authorized personnel 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.	Processes are in place to periodically review physical access to ensure consistency with job responsibilities.	Inspected the Physical Security Policy which states that Iterative reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually, to determine that processes are in place to periodically review physical access to ensure consistency with job responsibilities.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy, which states that production systems handling confidential data are required to have documented baseline configurations, when available, to determine that Iterative's Configuration and Asset Management Policy governs the configurations for new sensitive systems.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information.	Inspected the Access Control and Termination Policy which states that complex passwords are required for all users and multi-factor authentication is required for access to company email, version control tools, and cloud infrastructure, to determine that personnel are required to use strong, complex passwords and a second form of authentication to access sensitive systems, networks, and information. Moreover, inspected the Data Retention and Disposal Policy, to determine that Iterative allows only a limited number of employees to have access to customer data.	No exceptions noted.

CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	An Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	Inspected the Access Control and Termination Policy which defines the requirements for access and removal of access to Iterative data, systems, facilities, and networks, to determine that an Access Control and Termination Policy governs authentication and access to applicable systems, data, and networks.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Service data transmitted over the internet is encrypted-in-transit.	Inspected the Encryption and Key Management Policy which states that Iterative uses strong cryptography and security protocols (TLS 1.3 or a minimally TLS 1.1) to safeguard sensitive data during transmission over open, public networks, to determine that Iterative uses encryption to protect the transmission of data 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.	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, which provides guidance on the types of devices and media that need to be encrypted, when encryption must be used, and the minimum standards of the software used for encryption, to determine that Iterative has set out its requirements for generating and rotating, and storing cryptographic keys.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Descriptions of Iterative's services and systems are available to both internal personnel and external users.	Inspected the details of Iterative's solutions and products published on "https://iterative.ai/model-registry" and "https://iterative.ai/experiment-tracking" to determine that descriptions of Iterative's services are available to both internal personnel and external users.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected the Network Security Policy which states that Iterative utilizes threat monitoring solutions to detect and alert the management about network-based threats, 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 sources outside its system boundaries.	Configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	Inspected the Network Security Policy which states that Iterative requires networking ports and protocols to be restricted based on the least functionality principle, to determine that configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	No exceptions noted.
CC6.6	The entity implements logical access security	Logging and monitoring software is used to collect data from infrastructure to	Inspected the Information Security Policy, which states that Iterative uses logging solutions or SIEM tools to collect and monitor audit logs and	No exceptions noted.

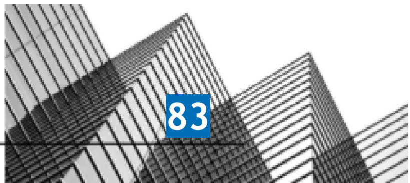
	measures to protect against threats from sources outside its system boundaries.	detect potential security threats, unusual system activity, and monitor system performance, as applicable.	alerts on key events stemming from production systems, applications, databases, servers, message queues, load balancers, and critical services as well as IAM user and admin activities, to determine that logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance.	
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 which defines the basic rules and requirements for network security and ensures the protection of information within and across networks and supporting information processing facilities, to determine that the Network Security Policy identifies the requirements for protecting information and systems within and across networks.	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.	Administrative access to production infrastructure is restricted based on the principle of least privilege.	Inspected the Access Control and Termination Policy which states that administrative access to production servers and databases is restricted based on the principle of least privilege for personnel who have a job function and business need for such access, to determine that administrative access to production infrastructure is restricted based on the principle of least privilege.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Service data is encrypted-at-rest.	Inspected the Configuration and Asset Management Policy which states that Iterative requires hard disks to be encrypted at rest by using FileVault for MacOS, LUKS for Linux, and Bitlocker for Windows operating systems, to determine that service data is encrypted at rest. Moreover, inspected the Encryption and Key Management Policy which states that Iterative requires data encryption at rest and shall only include strong encryption methods, to determine that Iterative is required to implement encryption-at-rest for service data.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and	Service data transmitted over the internet is encrypted-in-transit.	Inspected the Encryption and Key Management Policy which states that Iterative uses strong cryptography and security protocols (TLS 1.3 or a	No exceptions noted.



	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.		minimally TLS 1.1) to safeguard sensitive data during transmission over open, public networks, to determine that Iterative uses encryption to protect the transmission of data 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.	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, which provides guidance on the types of devices and media that need to be encrypted, when encryption must be used, and the minimum standards of the software used for encryption, to determine that Iterative has set out its requirements for generating and rotating, and storing cryptographic keys.	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 Acceptable Use Policy which states that Mobile Device Management (MDM) is implemented to manage and enforce mobile device configuration and security policies, including password policies, encryption, malware protection, and security updates, to determine that 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, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or	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 Iterative's Acceptable Use Policy which defines the standards for appropriate and secure use of Iterative's hardware and electronic systems including storage media, communication tools, and internet access, to determine that the Acceptable Use Policy is in place.	No exceptions noted.

	removal to meet the entity’s objectives.			
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.	A list of system assets, components, and respective owners are maintained and reviewed at least annually.	Inspected the Configuration and Asset Management Policy which states that Iterative inventories and tracks all assets that are used to process, store, transmit, or otherwise impact the confidentiality, integrity, or availability of sensitive information, and that Ken Thom or a designee will be held accountable for the accuracy of the inventory and must audit the asset list at least annually, to determine that Iterative maintains a list of Iterative's system components and owners and reviews it at least annually.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected the Configuration and Asset Management Policy which states that production systems handling confidential data must have documented baseline configurations, when available, to determine that baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.	System changes are approved by at least 1 independent person prior to deployment into production.	Inspected the Change Management Policy, which states that Iterative requires all new releases to be reviewed and approved by the appropriate product owner before being pushed to the production environment, to determine that system changes are approved by at least 1 independent person prior to deployment into production.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.	Development, staging, and production environments are segregated.	Inspected the Information Security Policy which states that Iterative maintains requirements and controls for the separation of the development and production environments, to determine that the production, development, and staging environments are segregated.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or	Production data is not used in the development and testing environments, unless required for debugging customer issues.	Inspected the Secure Development Policy which states that Iterative requires confidential and restricted data not to be used as test data, except where required for customer debugging, to determine that production data is not used in the development and testing environments.	No exceptions noted.

	malicious software to meet the entity's objectives.			
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy, which states that production systems handling confidential data are required to have documented baseline configurations, when available, to determine that Iterative's Configuration and Asset Management Policy governs the configurations for new sensitive systems.	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, which specifies that change management should be conducted according to a procedure that includes product road mapping, planning and evaluation, building, testing and documenting, reviewing the code, approval and implementation, communication, and post-change review, to determine that the Change Management Policy 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 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 Acceptable Use Policy which states that Mobile Device Management (MDM) is implemented to manage and enforce mobile device configuration and security policies, including password policies, encryption, malware protection, and security updates, to determine that company endpoints are managed and configured with a strong password policy, anti-virus, and hard drive encryption.	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 Iterative's Acceptable Use Policy which defines the standards for appropriate and secure use of Iterative's hardware and electronic systems including storage media, communication tools, and internet access, to determine that the Acceptable Use Policy is in place.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to	A list of system assets, components, and respective owners are maintained and reviewed at least annually.	Inspected the Configuration and Asset Management Policy which states that Iterative inventories and tracks all assets that are used to process, store, transmit, or otherwise impact the confidentiality, integrity, or availability of	No exceptions noted.

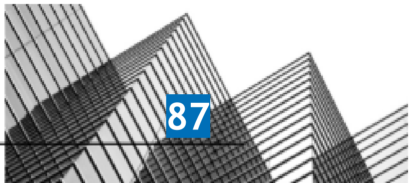


	identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		sensitive information, and that Ken Thom or a designee will be held accountable for the accuracy of the inventory and must audit the asset list at least annually, to determine that Iterative maintains a list of Iterative's system components and owners and reviews it at least annually.	
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected the Configuration and Asset Management Policy which states that production systems handling confidential data must have documented baseline configurations, when available, to determine that baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	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.	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy which states that the changes must be tested in an Iterative staging environment before the production release, to determine that software changes are tested before being deployed into production.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy, which states that production systems handling confidential data are required to have documented baseline configurations, when available, to determine that Iterative's Configuration and Asset Management Policy governs 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.	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected the Change Management Policy, which specifies that change management should be conducted according to a procedure that includes product road mapping, planning and evaluation, building, testing and documenting, reviewing the code, approval and implementation, communication, and post-change review, to determine that the Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan which provides guidelines for personnel to detect, report, and respond to incidents through to resolution, to determine that an Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected the Network Security Policy which states that Iterative utilizes threat monitoring solutions to detect and alert the management about network-based threats, to determine that security tools are implemented to provide monitoring of network traffic to the production environment.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the	Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.	Inspected the Information Security Policy, which states that Iterative uses logging solutions or SIEM tools to collect and monitor audit logs and alerts on key events stemming from production systems, applications, databases, servers, message queues, load balancers, and critical services as well as IAM user and admin activities, to determine that logging and monitoring	No exceptions noted.

	introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance.	
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 Information Security Policy which states that Iterative implements filters, parameters, and alarms to trigger alerts on logging events that deviate from the established system and activity baselines, to determine that alerting software is used to notify impacted teams of potential security events.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	A Vulnerability Management and Patch Management Policy outlines the processes to efficiently respond to identified vulnerabilities.	Inspected the Vulnerability Management and Patch Management Policy which states that Iterative schedules third-party security assessments and penetration test and vulnerability scan results to verify vulnerabilities and analyze their impact, to determine that a Vulnerability Management and Patch Management Policy 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.	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected the Vulnerability and Patch Management Policy which states that Iterative periodically tests the security posture of its applications and systems through third-party testing and vulnerability scanning, to determine that vulnerability scanning is performed on production infrastructure systems regularly.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection	A 3rd party is engaged to conduct a network and application penetration	Inspected the Vulnerability and Patch Management Policy which states that Iterative schedules third-party penetration tests at least	No exceptions noted.

	and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	annually to determine that a third party is engaged to conduct a network and application penetration test of the production environment at least annually.	
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.	Physical protections are in place to safeguard facilities, infrastructure, systems, and data from external and internal threats.	Inspected the Physical Security Policy which specifies the requirements for physically protecting assets and their data via physical controls and safeguards, to determine that physical protections are in place to safeguard facilities, infrastructure, systems, and data from external and internal threats.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan which provides guidelines for personnel to detect, report, and respond to incidents through to resolution, to determine that an Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters,	Security tools are implemented to provide monitoring of network traffic to the production environment.	Inspected the Network Security Policy which states that Iterative utilizes threat monitoring solutions to detect and alert the management about network-based threats, to determine that security tools are implemented to provide monitoring of network traffic to the production environment.	No exceptions noted.



	and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine 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.	Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.	Inspected the Information Security Policy, which states that Iterative uses logging solutions or SIEM tools to collect and monitor audit logs and alerts on key events stemming from production systems, applications, databases, servers, message queues, load balancers, and critical services as well as IAM user and admin activities, to determine that logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance.	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 which defines the basic rules and requirements for network security and ensures the protection of information within and across networks and supporting information processing facilities, to determine that the Network Security Policy identifies the requirements for protecting information and systems within and across networks.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts,	A continuous monitoring solution monitors internal controls used in the achievement of service commitments and system requirements.	Inspected the Internal Control Policy, which states that Iterative manages and maintains its internal controls using the Secureframe platform, to determine that a continuous monitoring solution monitors the internal controls used in the achievement of service commitments and system requirements.	No exceptions noted.

	natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2	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.	Physical protections are in place to safeguard facilities, infrastructure, systems, and data from external and internal threats.	Inspected the Physical Security Policy which specifies the requirements for physically protecting assets and their data via physical controls and safeguards, to determine that physical protections are in place to safeguard facilities, infrastructure, systems, and data from external and internal threats.	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.	Production data is not used in the development and testing environments, unless required for debugging customer issues.	Inspected the Secure Development Policy which states that Iterative requires confidential and restricted data not to be used as test data, except where required for customer debugging, to determine that production data is not used in the development and testing environments.	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	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy, which states that production systems handling confidential data are required to have documented baseline configurations, when available, to determine that Iterative's Configuration and Asset Management Policy governs the configurations for new sensitive systems.	No exceptions noted.

	address such failures.			
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Terms of Service or the equivalent are published or shared to external users.	Inspected the Privacy & Cookie Policy of Iterative published on "https://iterative.notion.site/Privacy-Cookie-Policy-edbce9b3b3d14f26950b7dca617b2033", which states the data use and disclosure policies, to determine that Terms of Service or the equivalent are published or shared to external users.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	A Privacy Policy to both external users and internal personnel. This policy details Iterative's privacy commitments.	Inspected the Privacy & Cookie Policy of Iterative published on "https://iterative.notion.site/Privacy-Cookie-Policy-edbce9b3b3d14f26950b7dca617b2033" which describes the steps taken by Iterative to ensure data privacy, to determine that Iterative publishes its Privacy Policy to both external users and internal personnel and states its privacy commitments.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan which provides guidelines for personnel to detect, report, and respond to incidents through to resolution, to determine that an Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through 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	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inspected the Internal Control Policy which states that Iterative requires all issues that impact internal control to be tracked and monitored until the resolution is implemented, to determine that identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	No exceptions noted.

	actions to prevent or address such failures.			
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance, as applicable.	Inspected the Information Security Policy, which states that Iterative uses logging solutions or SIEM tools to collect and monitor audit logs and alerts on key events stemming from production systems, applications, databases, servers, message queues, load balancers, and critical services as well as IAM user and admin activities, to determine that logging and monitoring software is used to collect data from infrastructure to detect potential security threats, unusual system activity, and monitor system performance.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Alerting software is used to notify impacted teams of potential security events.	Inspected the Information Security Policy which states that Iterative implements filters, parameters, and alarms to trigger alerts on logging events that deviate from the established system and activity baselines, to determine that alerting software is used to notify impacted teams of potential security events.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Physical protections are in place to safeguard facilities, infrastructure, systems, and data from external and internal threats.	Inspected the Physical Security Policy which specifies the requirements for physically protecting assets and their data via physical controls and safeguards, to determine that physical protections are in place to safeguard facilities, infrastructure, systems, and data from external and internal threats.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy which states that the changes must be tested in an Iterative staging environment before the production release, to determine that software changes are tested before being deployed into production.	No exceptions noted.

	communicate security incidents, as appropriate.			
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Production data is not used in the development and testing environments, unless required for debugging customer issues.	Inspected the Secure Development Policy which states that Iterative requires confidential and restricted data not to be used as test data, except where required for customer debugging, to determine that production data is not used in the development and testing environments.	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.	Terms of Service or the equivalent are published or shared to external users.	Inspected the Privacy & Cookie Policy of Iterative published on "https://iterative.notion.site/Privacy-Cookie-Policy-edbce9b3b3d14f26950b7dca617b2033", which states the data use and disclosure policies, to determine that Terms of Service or the equivalent are published or shared to external users.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan which provides guidelines for personnel to detect, report, and respond to incidents through to resolution, to determine that an Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	Inspected the Internal Control Policy which states that Iterative requires all issues that impact internal control to be tracked and monitored until the resolution is implemented, to determine that identified incidents are documented, tracked, and analyzed according to 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.	After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve company security and operations.	Inspected the Change Management Policy which states that an appropriate team must discuss and document any lessons learned during the security incident response with the product management and other appropriate team members, to determine that Iterative requires a 'Lessons Learned' document.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The Incident Response Plan is periodically tested via tabletop exercises or equivalents. When necessary, Management makes changes to the Incident Response Plan based on the test results.	Inspected the Information Security Policy which states that annual testing of the Incident Response Plan may be performed using walkthroughs and tabletop exercises and any gaps in the plan that are discovered during the testing phase should be addressed by the management, to determine that the Incident Response Plan is periodically tested.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Alerting software is used to notify impacted teams of potential security events.	Inspected the Information Security Policy which states that Iterative implements filters, parameters, and alarms to trigger alerts on logging events that deviate from the established system and activity baselines, to determine that alerting software is used to notify impacted teams of potential security events.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	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 and Code of Conduct which state that any violation of Iterative policies or procedures may result in disciplinary action, up to and including termination of employment, to determine that personnel who violate information security policies are subject to disciplinary action and such disciplinary action is documented in one or more policies.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by	Vulnerability scanning is performed on production infrastructure systems, and	Inspected the Vulnerability and Patch Management Policy which states that Iterative periodically tests the security posture of its	No exceptions noted.

	executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	identified deficiencies are remediated on a timely basis.	applications and systems through third-party testing and vulnerability scanning, to determine that vulnerability scanning is performed on production infrastructure systems regularly.	
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	A 3rd party is engaged to conduct a network and application penetration test of the production environment at least annually. Critical and high-risk findings are tracked through resolution.	Inspected the Vulnerability and Patch Management Policy which states that Iterative schedules third-party penetration tests at least annually to determine that a third party is engaged to conduct a network and application penetration test of the production environment at least annually.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Terms of Service or the equivalent are published or shared to external users.	Inspected the Privacy & Cookie Policy of Iterative published on "https://iterative.notion.site/Privacy-Cookie-Policy-edbce9b3b3d14f26950b7dca617b2033", which states the data use and disclosure policies, to determine that Terms of Service or the equivalent are published or shared to external users.	No exceptions noted.
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 Internal Control Policy which states that Iterative requires all issues that impact internal control to be tracked and monitored until the resolution is implemented, to determine that identified incidents are documented, tracked, and analyzed according to the Incident Response Plan.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	After any identified security incident has been resolved, management provides a "Lessons Learned" document to the team in order to continually improve company security and operations.	Inspected the Change Management Policy which states that an appropriate team must discuss and document any lessons learned during the security incident response with the product management and other appropriate team members, to determine that Iterative requires a 'Lessons Learned' document.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover	The Incident Response Plan is periodically tested via tabletop exercises or equivalents. When	Inspected the Information Security Policy which states that annual testing of the Incident Response Plan may be performed using walkthroughs and tabletop exercises and any	No exceptions noted.

	from identified security incidents.	necessary, Management makes changes to the Incident Response Plan based on the test results.	gaps in the plan that are discovered during the testing phase should be addressed by the management, to determine that the Incident Response Plan is periodically tested.	
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	Inspected the Configuration and Asset Management Policy which states that production systems handling confidential data must have documented baseline configurations, when available, to determine that baseline configurations and codebases for production infrastructure, systems, and applications are securely managed.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Software changes are tested prior to being deployed into production.	Inspected the Change Management Policy which states that the changes must be tested in an Iterative staging environment before the production release, to determine that software changes are tested before 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.	System changes are approved by at least 1 independent person prior to deployment into production.	Inspected the Change Management Policy, which states that Iterative requires all new releases to be reviewed and approved by the appropriate product owner before being pushed to the production environment, to determine that system changes are approved by at least 1 independent person prior to deployment into production.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and	Development, staging, and production environments are segregated.	Inspected the Information Security Policy which states that Iterative maintains requirements and controls for the separation of the development and production environments, to determine that the production, development, and staging environments are segregated.	No exceptions noted.

	procedures to meet its objectives.			
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Production data is not used in the development and testing environments, unless required for debugging customer issues.	Inspected the Secure Development Policy which states that Iterative requires confidential and restricted data not to be used as test data, except where required for customer debugging, to determine that production data is not used in the development and testing 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.	A Configuration and Asset Management Policy governs configurations for new sensitive systems.	Inspected the Configuration and Asset Management Policy, which states that production systems handling confidential data are required to have documented baseline configurations, when available, to determine that Iterative's Configuration and Asset Management Policy governs 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.	A Change Management Policy governs the documenting, tracking, testing, and approving of system, network, security, and infrastructure changes.	Inspected the Change Management Policy, which specifies that change management should be conducted according to a procedure that includes product road mapping, planning and evaluation, building, testing and documenting, reviewing the code, approval and implementation, communication, and post-change review, to determine that the Change Management Policy 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.	A Secure Development Policy defines the requirements for secure software and system development and maintenance.	Inspected the Secure Development Policy which states that Oded Messer issues procedures for secure information system engineering practices for the development of new systems and for the maintenance of the existing systems, to determine that Iterative has defined the requirements for secure software and system development and maintenance.	No exceptions noted.

CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	Inspected the Network Security Policy which states that Iterative requires networking ports and protocols to be restricted based on the least functionality principle, to determine that configurations ensure available networking ports, protocols, services, and environments are restricted as necessary, including firewalls.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Senior management and/or board of directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. The information security team meets at least annually to discuss security risks, roles & responsibilities, controls, changes, audit results and/or other matters as necessary.	Inspected the bylaws of Iterative which state that the Board manages the business and affairs of Iterative, directly or by delegating authority to committees and officers as provided by the bylaws, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters. Moreover, inspected the minutes of a telephonic meeting of the Board held on August 22, 2022, to determine that the Board of Directors meets at least annually to review business goals, company initiatives, resource needs, risk management activities, and other internal/external matters.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Vulnerability scanning is performed on production infrastructure systems, and identified deficiencies are remediated on a timely basis.	Inspected the Vulnerability and Patch Management Policy which states that Iterative periodically tests the security posture of its applications and systems through third-party testing and vulnerability scanning, to determine that vulnerability scanning is performed on production infrastructure systems regularly.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	An Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution.	Inspected the Security Incident Response Plan which provides guidelines for personnel to detect, report, and respond to incidents through to resolution, to determine that an Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.	No exceptions noted.

CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Cybersecurity insurance has been procured to help minimize the financial impact of cybersecurity loss events.	Inspected the Risk Assessment and Treatment Policy which states that Iterative considers purchasing insurance as an appropriate form of risk transfer, to determine that cybersecurity insurance may be 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.	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 which describes the risk assessment framework and process, to determine that Iterative has a process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners.	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, and fraud, and an analysis of risks associated with those threats.	Inspected the Risk Assessment and Treatment Policy, which states that Iterative follows a risk assessment framework and process for identifying, analyzing, scoring, and mitigating risks, and that risk assessments must be conducted at least annually or whenever there are significant changes to Iterative or its systems, to determine that formal risk assessments are performed.	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 of Iterative maintained on Secureframe, identifying 4 risks with an assigned risk owner, 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.
CC9.2	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 which states provides a framework for the onboarding, assessment, and management of the vendor relationship lifecycle, including due diligence, risk assessment, contract review, and security controls, to determine that the policy defines a framework for the onboarding and management of the vendor relationship lifecycle.	No exceptions noted.

CC9.2	The entity assesses and manages risks associated with vendors and business partners.	New vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor. Reassessment occurs at least annually.	Inspected the Vendor Management Policy which states that a risk assessment and appropriate due diligence shall be performed for new vendors, to determine that new vendors are assessed in accordance with the Vendor Risk Management Policy prior to engaging with the vendor.	No exceptions noted.