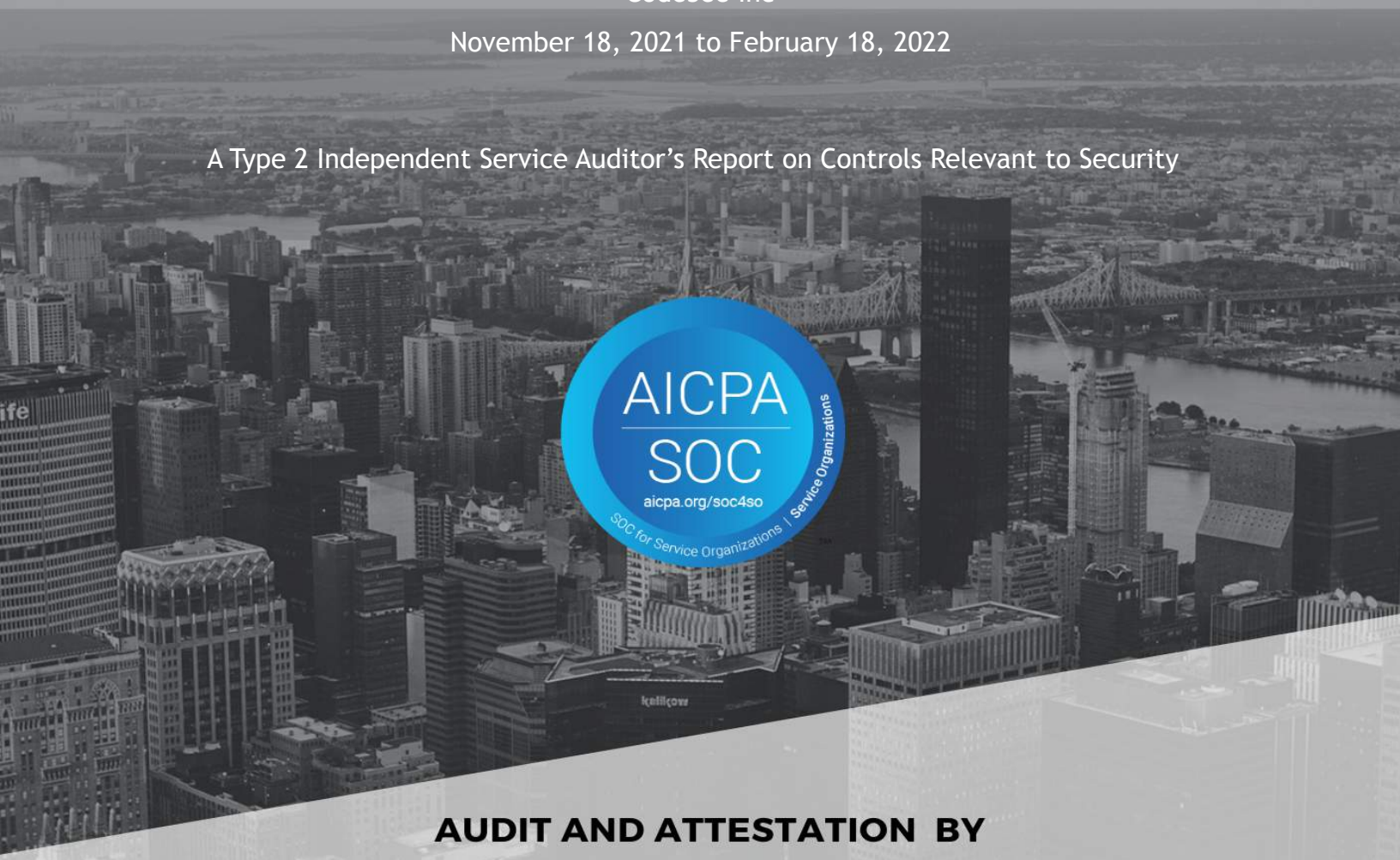
CodeSee

SOC 2 Type 2 Report

CodeSee Inc

November 18, 2021 to February 18, 2022

A Type 2 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

AICPA NOTICE:

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

TABLE OF CONTENTS

TABLE OF CONTENTS

SECTION 1

Management's Assertion

Management's Assertion

We have prepared the accompanying description of CodeSee Inc's system throughout the period November 18, 2021, to February 18, 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 CodeSee Inc's system that may be useful when assessing the risks arising from interactions with CodeSee Inc's system, particularly information about system controls that CodeSee Inc has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

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

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

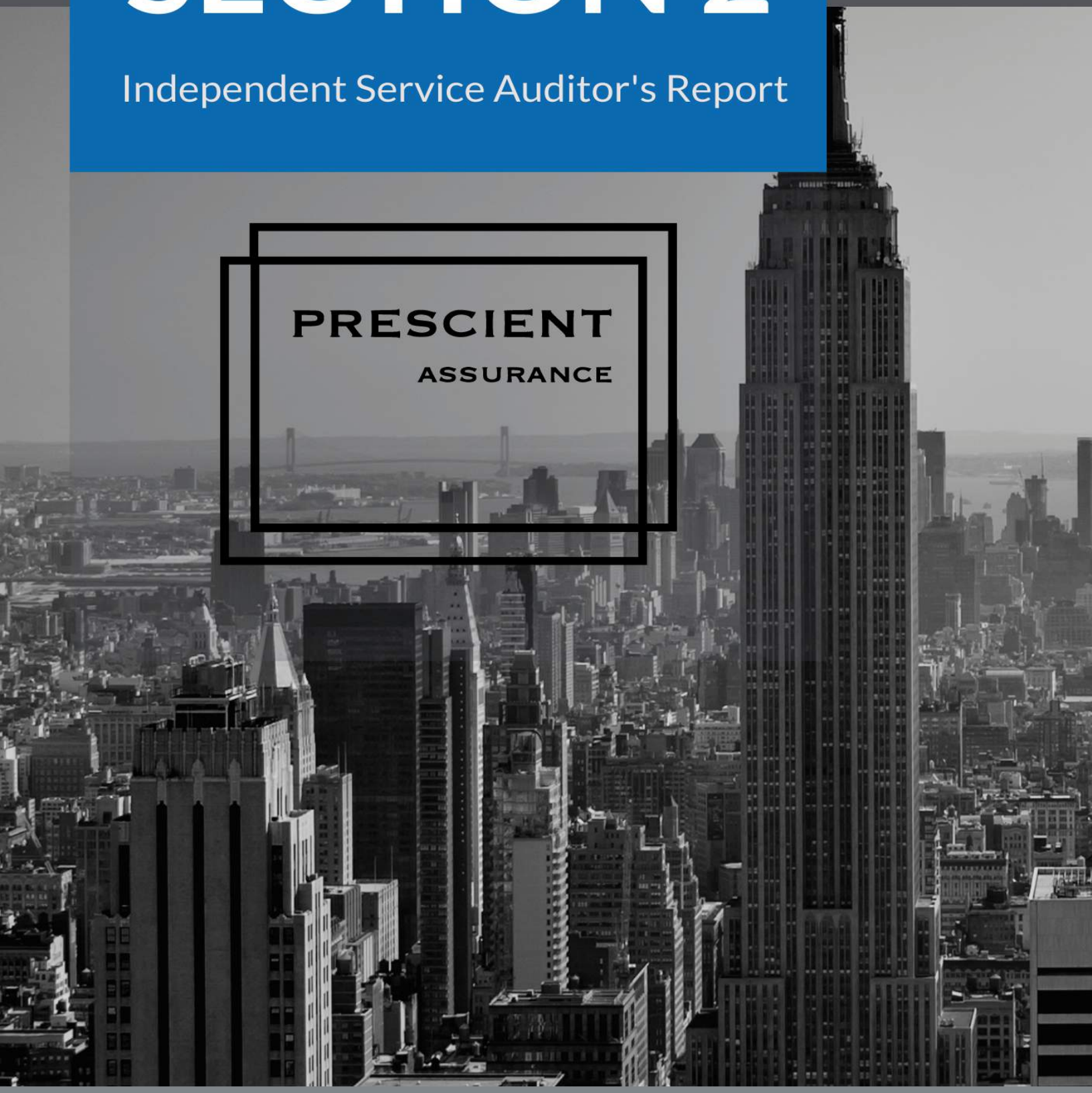
a. The description presents CodeSee Inc's system that was designed and implemented throughout the period November 18, 2021, to February 18, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period November 18, 2021, to February 18, 2022, to provide reasonable assurance that CodeSee Inc's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of CodeSee Inc's controls during that period.

c. The controls stated in the description operated effectively throughout the period November 18, 2021, to February 18, 2022, to provide reasonable assurance that CodeSee Inc's service commitments and system requirements were achieved based on the applicable trust services criteria, and if the subservice organization and user entities applied the complementary controls assumed in the design of CodeSee Inc's controls operated effectively throughout the period.

Shanea Leven
CEO OF CodeSee Inc

SECTION 2

Independent Service Auditor's Report



Independent Service Auditor's Report

To: CodeSee Inc

Scope

We have examined CodeSee Inc's ("CodeSee Inc") accompanying description of its CodeSee system in Section 3 titled CodeSee Inc System Description throughout the period November 18, 2021, to February 18, 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 and operating effectiveness of controls stated in the description throughout the period November 18, 2021, to February 18, 2022, to provide reasonable assurance that CodeSee 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.

CodeSee 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 CodeSee Inc, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents CodeSee Inc's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CodeSee Inc's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

CodeSee 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 CodeSee Inc's service commitments and system requirements were achieved. In Section 1, CodeSee Inc has provided the accompanying assertion titled "Management's Assertion of CodeSee Inc" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. CodeSee Inc is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the

related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

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

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

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

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

Inherent Limitations

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

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

Opinion

In our opinion, in all material respects:

a. The description presents CodeSee Inc's system that was designed and implemented throughout the period November 18, 2021, to February 18, 2022, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period November 18, 2021, to February 18, 2022, to provide reasonable assurance that CodeSee Inc's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of CodeSee Inc's controls throughout the period.
c. The controls stated in the description operated effectively throughout the period November 18, 2021, to February 18, 2022, to provide reasonable assurance that CodeSee Inc's service commitments and system requirements were achieved based on the applicable trust services criteria, and if subservice organization and user entity complementary controls assumed in the design of CodeSee Inc's controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of CodeSee Inc, user entities of CodeSee Inc's system during some or all of the period **November 18, 2021, to February 18, 2022**, business partners of CodeSee Inc subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

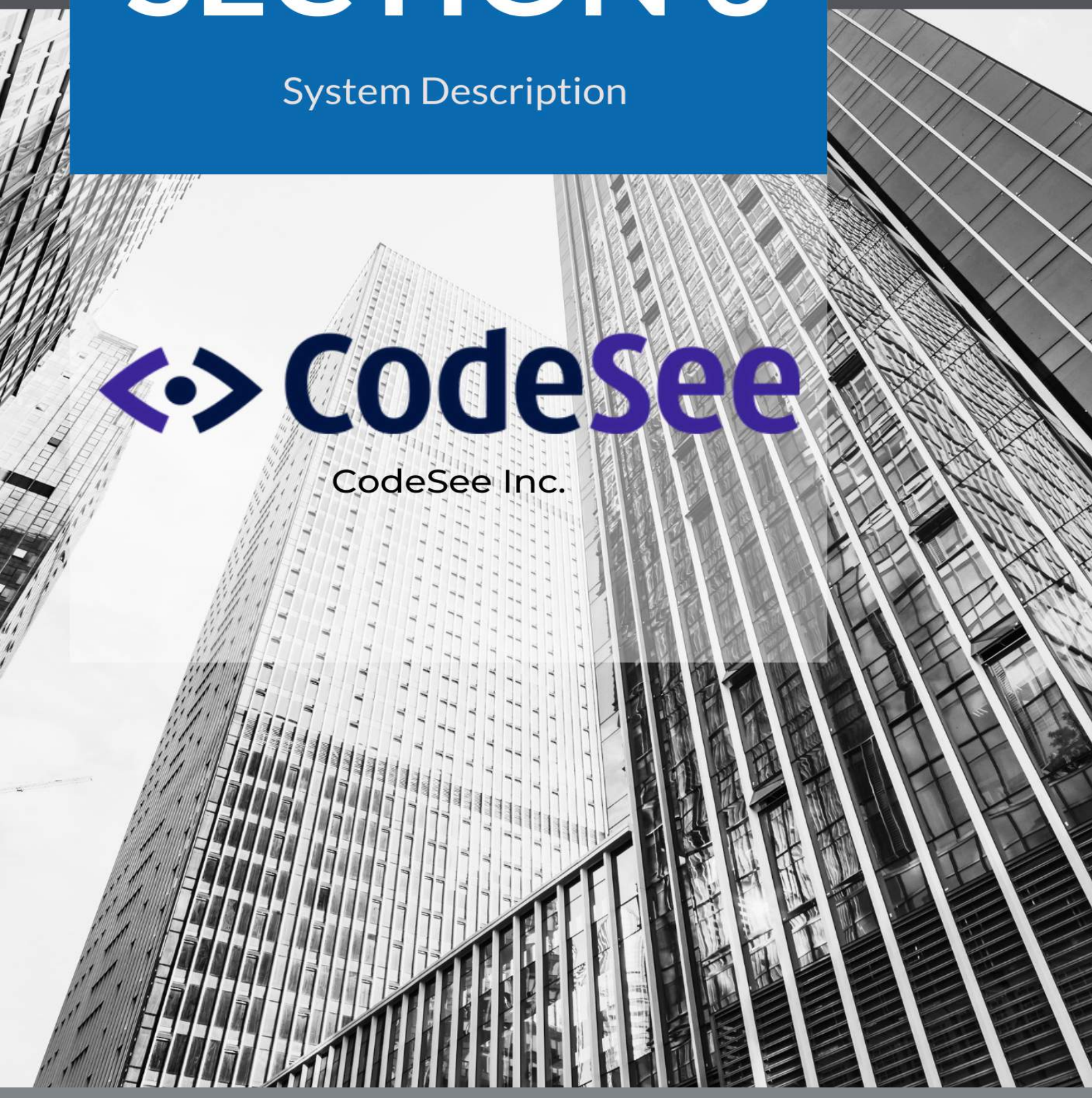
Prescient Assurance LLC

_____

John D. Wallace, CPA
Signal Mountain, TN
February 22, 2022

SECTION 3

System Description



CodeSee

CodeSee Inc.

DC 1: Company overview and types of products and services provided

CodeSee is a developer tools company that offers code understanding services to software companies using its SAAS platform or expert resources. We make it easier for developers to understand and communicate about their code by analyzing that code and related data sets and creating interactive visualizations. CodeSee was founded in 2019. We have users across the globe but no paying customers at this time.

CodeSee provides:

- ***CodeSee Maps:*** Providing software companies and developers with codebase analysis tools, integrated with GitHub. Users add the CodeSee Github workflows to their codebase, those workflows run analyses on their code as it changes, and our SaaS platform turns those analyses into interactive visualizations on app.codesee.io.
- ***CodeSee Recordings:*** Libraries that are integrated into a Javascript or Typescript build system, automatically add instrumentation to that code, and allow the user to generate recordings of their code at runtime, then transmit those recordings to our SaaS platform and turn into an interactive visualization for deeper understanding.

DC 2: The principal service commitments and system requirements

CodeSee designs its processes and procedures to meet the objective of increasing developer productivity. That objective is based on the service commitments that CodeSee makes to user entities, the laws and regulations that govern the provision of services, and the financial, operational, and compliance requirements that CodeSee has established for the services. The services of CodeSee are subject to the federal and state privacy and security laws and regulations in the jurisdictions in which CodeSee operates.

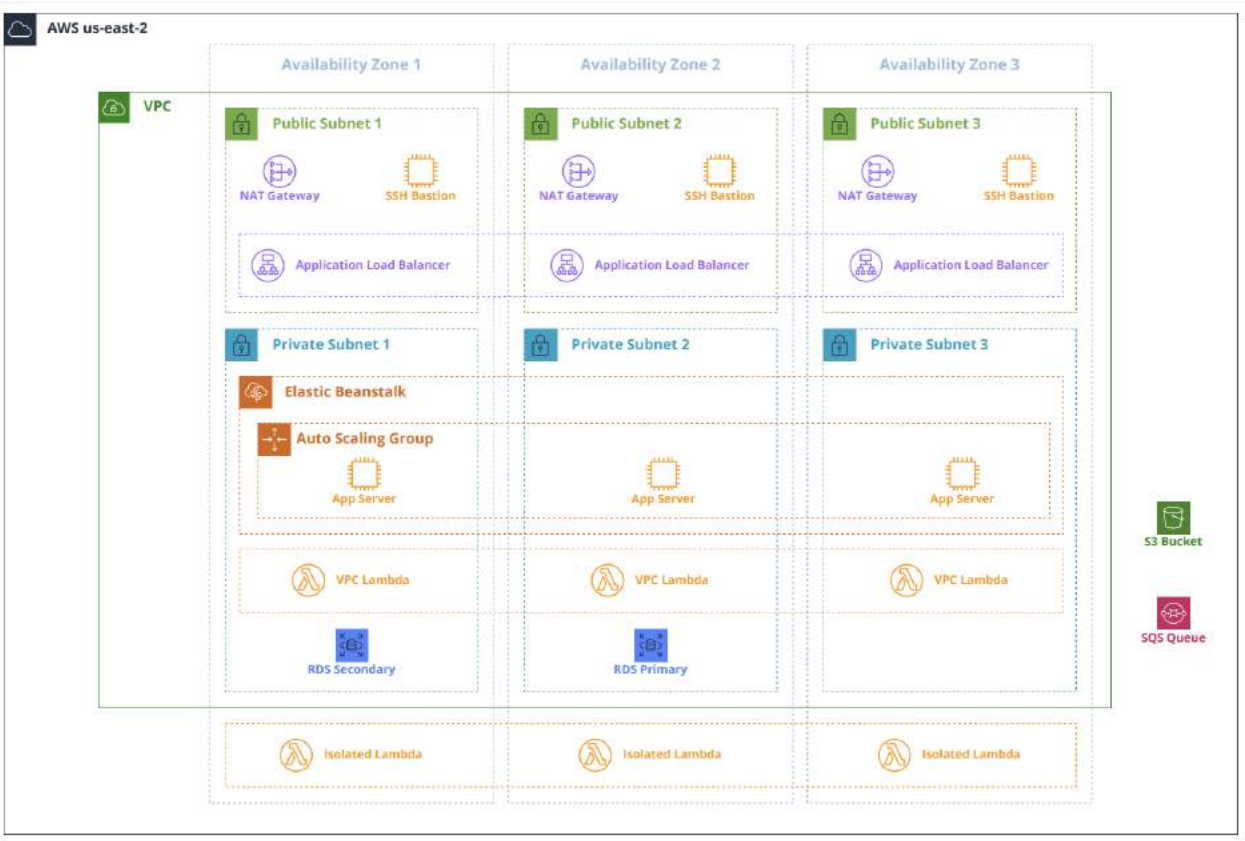
Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online. More details at docs.codesee.io. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the CodeSee platform that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Maintain commercially reasonable administrative, technical, and organizational measures that are designed to protect customer data processed.
- Encryption of data at rest and in transit.
- Maintain security procedures that are consistent with applicable industry standards.
- Document and enforce confidentiality agreements with third parties prior to sharing confidential data.
- Review documentation from third-party providers to help ensure that they are in compliance with security and confidentiality policies.
- Maintain business continuity and disaster recovery programs.
- Restrict system access to authorized personnel only.
- Regularly assess security programs and processes.
- Identification and remediation of security incidents/events.

CodeSee establishes systems and operational requirements that support the achievement of service commitments, relevant laws and regulations, and other security and privacy requirements. Such requirements are communicated in CodeSee's Terms and Conditions and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system s operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the CodeSee Platform.

DC 3: The components of the system used to provide the services

Primary Infrastructure



Primary Infrastructure		
Hardware	**Type**	**Purpose**

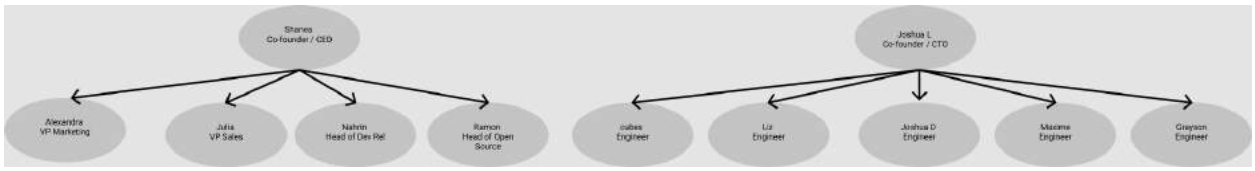
AWS	VPCs EC2 Instances IAM Load Balancers	Allow for the servicing, processing, and directing of network traffic and data. Allow management of user accounts.
AWS	S3 Buckets	Cloud-hosted storage solution with encryption capabilities used to store objects created during development and business operations i.e. artifacts, user avatars, authentication files, and CloudTrail logs.
AWS	CloudWatch/CloudTrail	Used for monitoring network resources and alerting based on preconfigured metric-based alarms.
AWS	RDS Instances	Used to store user and customer data.
GitHub	Codebase & CICD/Pipeline	Codebase used for versioning, testing, and deployment of changes to the environments.
Jira/Coda	Communication Services	Internal business communications, storage of organizational documents, and project management.
AWS Inspector	Vulnerability Scanning	Monitors infrastructure for common vulnerabilities and aids in ensuring compliance.
Docker Hub	Container repository hosting service	Repository for all product containers
DataDog	Observability/Logs Aggregation	Application logs for all of the services Error detection and alerting for software issues

Okta	User Management	Handles our end-user authentication

Primary Software

Primary Software		
Software	**Type**	**Purpose**
NodeJS	Server Side Logic	Primary development language/runtime for all applications
ReactJS	UI Logic	Web application framework used to power the web application
AWS Lambda	Functions	Background worker platform
PostgreSQL	Database	Transactional database for customer data
AWS SQS	Queues	Queue management software for job queue.
Debian Stretch	Operating System	Base of our Docker images
Amazon Linux 2	Operating System	OS of our host instances
Nginx	Reverse Proxy	Reverse proxy for our primary application

People



CodeSee has a staff of approximately 13 employees and contractors organized in the following functional areas:

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

- **Product Development:** Product managers and software engineers who design and maintain the CodeSee Platform, including the web interface, the APIs, the databases, and the integrations with data sources. This team designs and implements new functionality, assesses, and remediates any issues or bugs found in the CodeSee Platform, and architects and deploys the underlying cloud infrastructure on which the platform runs. Members of the product team are responsible for peer reviews of code and infrastructure designed and authored within the team. This includes DevOps responsibilities such as maintaining the cloud infrastructure that the CodeSee product runs on. This also includes security: providing ongoing security to CodeSee's assets (people, application, infrastructure, and data).
- **Go-to-market:** Individuals responsible for building and maintaining developer community, creating content, and marketing.
- **Sales:** Individuals responsible for customer acquisition.

Processes and Procedures

The Company employs a set of procedures in order to obtain its objectives for network and data security. These procedures are executed by qualified and experienced team members. Procedures are in place in the following areas:
CodeSee application runs in the AWS Cloud.

- The production platform instance is contained within a separate AWS Elastic Beanstalk project. The project infrastructure provides granular access control to all aspects of the infrastructure. Access from external locations is controlled through configuration and firewall rules. Access to internal components of the platform is only possible via access utilizing the Secure Shell ("SSH") protocol. Access is granted on a project and component within each project (i.e., pods, storage, and database) basis.
- We do not maintain a long-running staging environment but bring one up in a separate and isolated AWS Elastic Beanstalk environment as needed.
- Data is persisted in both AWS Storage and Postgres Services. Both utilize Advanced Encryption Standard ("AES") 256 encrypted disks for all data stored at rest.
- User entities access the service using standard web browsers utilizing Transport Service License ("TSL") 1.2 or above for encrypted communications.

- *Security Policy Administration:* The Company's policies concerning various security, availability, processing integrity, confidentiality, and privacy matters are reviewed at least annually by the Security Team.
- *Risk Assessment:* At least annually the Chief Executive, Development, Security, and IT Teams collaborate on an overall risk assessment for the Company and the System.
- *Communication:* The Company opportunistically and continually uses a mixture of intranet services, email, and zoom meeting opportunities for the communication of security policies and procedures. Regular confirmation of this communication is captured in annual attestations from each team member that they have read general internal policies.
- *Logical Access:* All team members must have unique credentials as well as established authorization to access the Company's information assets. Access to systems and information is restricted based on the responsibilities of the individual and their role.
- *Change Management:* The Company has a Secure Development Policy. The Policy covers the planning, assignment, development, design, code review, impact considerations, infrastructure

assignments, quality assurance, security testing, implementation, and maintenance of both the System software and infrastructure.

Data

These are four major types of data used by CodeSee.

Principal Data Types	
Data Types	**Protection and Breach Notification during the lifecycle of Data**
Configuration Data: Data used to configure CodeSee System	Configuration Data is stored in a PostgreSQL database and includes the names of GitHub code repositories and code workspaces. It is encrypted at rest with AES 256 and uses TLS for communication on the wire.
Customer Data: Data owned by CodeSee's customers that is copied from edge compute devices to web-based software application	Customer Data is stored in PostgreSQL databases, and includes customer application execution traces captured and stored by the CodeSee System. It is encrypted at rest with AES 256 and uses TLS for communication on the wire. Only authorized CodeSee operators are permitted to access customer data and only for justifiable business use cases, such as debugging failures, machine learning training problems, or other operational issues. CodeSee further encrypts CodeSee API tokens using cryptographic hash functions and tokens provided by integrations (e.g. GitHub) using PGP symmetric encryption.
Log Data: Logs produced by the CodeSee System	Log Data is produced by the various services to make it easier for CodeSee operators to monitor the health of the system and track down any issues. Log data may be stored by vendors that CodeSee has entrusted for purposes like indexing, monitoring, and trending. Log data is retained for at least one year.
Service Data	Service Data is user and account metadata, troubleshooting, accounts receivable and billing, and related information necessary for the Company to know in order to service accounts and provide the Service.
Data in transit	To protect data in transit between our app and our servers, CodeSee supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS 1.2 protocols, AES256 encryption, and SHA2 signatures, whenever supported by the clients.
Data at rest	Data at rest in CodeSee's production network is encrypted using industry-standard 256-bit Advanced Encryption Standard (AES256), which applies to all types of data at rest within CodeSee's systems—relational databases, file stores, database backups, etc.

System Boundaries

The following systems are not within the boundaries of the description of the system in scope:

None.

Third-Party Access

There are no third-party vendors with any level of privileges to our services.

DC 4: Disclosures about identified security incidents

Name of incident	Timing	Impact
N/A	N/A	N/A

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

Integrity and Ethical Values

CodeSee uses its Code of Conduct, which is read and signed by all employees as part of the onboarding process, to define and lay out our values. CodeSee has also instituted a number of technical controls to prevent and disincentivize illegal and unethical actions by CodeSee employees. These controls include but are not limited to:

- Logging all traffic within CodeSee's network by user for full traceability.
- Limiting access to confidential information based on clearly defined roles and following the principle of least privilege.
- Rigorously upholding the standards of ethical behavior laid out in our Code of Conduct especially as they pertain to discrimination and harassment of any kind.
- Performing background checks on domestic employees as part of the hiring process.
- Protecting and valuing individuals who bring concerns to the attention of CodeSee management.
- Use of NDAs to prevent the disclosure of confidential information to unauthorized parties.

Commitment to Competence

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

Specific control activities that have been implemented in this area are described below:

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

Management's Philosophy and Operating Style

CodeSee's management team is committed to creating a productive and encouraging work environment as well as providing a secure product to our customers and users. To accomplish this CodeSee has instituted a number of processes:

- Weekly “retrospective” meetings for each team to voice things we should continue, start and stop.
- Monthly “all hands” meetings for employees to voice their blocks, successes, and concerns.
- A rigorous QA program ensuring that development on the CodeSee application meets industry security standards.
- Meetings are held between managers on a weekly basis to prioritize objectives and tasks.
- Employees are encouraged to reach out to each other when facing obstacles.

Organizational Structure and Assignment of Authority and Responsibility

During normal operations CodeSee has a simple organizational structure. Engineers report to the CTO. All other employees (including the CTO) report directly to the CEO. CodeSee has clearly defined job descriptions and as the organization grows we have in place roles and responsibilities which will allow for the dissemination of managerial responsibilities as necessary. CodeSee has taken the following steps to achieve this goal:

- Regularly updated organization chart fully accessible by employees.
- Responsibilities of roles are clearly defined in policies and job descriptions.

Human Resource Policies and Practices

CodeSee consistently strives to hire and retain the most qualified individuals for the job. To meet this goal, CodeSee has in place onboarding requirements and a Human Resource Security Policy which cover employee security training, performance reviews, competency assessments, and the terms of employment.

Specifically, CodeSee has the following controls in place:

- Annual Performance Reviews
- Annual employee security training
- New employees are required to sign a non-disclosure or confidentiality agreement.
- Clearly defined disciplinary process
- A “New Employee Checklist” is given to new hires and is fully accessible to all CodeSee employees
- Lastly, CodeSee recognizes that policies and procedures often need to change to serve the needs of the organization. To accomplish this, all security procedures are reviewed at least annually.

Security Management

CodeSee’s CTO leads all efforts related to information security and is responsible for the management of information security throughout the organization. The CTO is ultimately responsible for, and with help from the engineering team, maintains security credentials, performs the technical onboarding/off-boarding work, and updates, maintains, and annually signs to acknowledge their review of the information security policies. The CTO is responsible for enforcing the information security

policies, configuring, monitoring, and maintaining preventative, corrective, and detective controls within the CodeSee environment, and ensuring user awareness training is conducted.

As the CTO maintains security, they monitor known incidents and patches as well as results from recent vulnerability assessments and address necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly planning meetings or through system alerts.

During annual security training and awareness programs, management ensures communication of the latest security policies as well as written job descriptions for security management.
Additionally, management is responsible for ensuring business associate agreements are current for third parties and for updating the annual IT risk assessment.

Security Policies

CodeSee has adopted the following Security Policies:

- Acceptable Use Policy
- Access Control and Termination Policy
- Business Continuity and Disaster Recovery Plan
- Change Management Policy
- Code of Conduct
- Configuration and Asset Management Policy
- Data Classification Policy
- Data Retention and Disposal Policy
- Encryption and Key Management Policy
- Information Security Policy
- Internal Control Policy
- Network Security Policy
- Performance Review Policy
- Physical Security Policy
- Risk Assessment and Treatment Policy
- Secure Development Policy
- Security Incident Response Plan
- Vendor Management Policy
- Vulnerability and Patch Management Policy

Personnel Security

CodeSee has several personnel security procedures in place specifically during the onboarding process. These include:

- Background checks for new domestic employees.
- Employees must read and agree to all security policies.
- Roles within the organization have been clearly defined and are reflected in the organizational chart.

- Employees are granted access/authorization based on their role and in accordance with the principle of least privilege.
- Employees are required to sign an NDA.
- Upon hire and annually thereafter. security awareness training is completed by all CodeSee employees.
- Employees are directed to report any potential security incidents to the IT Manager.
- Violations of CodeSee security policies have clearly defined repercussions.

Physical Security and Environmental Controls

CodeSee 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 Policy, our Business Continuity and Disaster Recovery Plan, and our Information Security Policy.

Change Management

CodeSee's change management procedures are detailed in the Change Management Policy. All change requests must be documented end-to-end via the CodeSee change management and ticketing tools. Change management should be conducted according to the following procedure (barring any exceptions as noted in the Policy):

1. **Product Roadmap** - All change requests should be prioritized in terms of benefits, urgency, the effort required, security impacts, and other potential impacts on the organization's operations by the CodeSee product management team.
2. **Planning and Evaluation** - This may include design, scheduling, and implementation of a communications plan, testing plan, and roll-back plan.
3. **Build, Test, and Document** - The changes must be tested before release to production. Automated test scripts should be developed, used, and updated as changes occur.
4. **Code Review** - Code reviewers should look at design, functionality, complexity, tests, security, naming, comments, style, and documentation.
5. **Approval and Implementation** - Once the new release is ready and the appropriate documentation is in place, the new release may be pushed to the production environment after the appropriate review and approval by the appropriate product owner.
6. **Communication** - Implemented changes should be communicated to all applicable team members and externally as appropriate.
7. **Post-Change Review** - The appropriate team may conduct a post-implementation review to determine how the change is impacting CodeSee and our customers, either positively or negatively.

System Monitoring

CodeSee uses a combination of services to monitor its network and systems. These include Datadog Logs for aggregation, AWS CloudTrail, AWS GuardDuty, AWS S3 access logs, AWS ELB access logs, AWS Inspector findings.

- Datadog Metrics/CloudWatch: Used for monitoring of network usage, availability, and overall performance and health of network resources.
- AWS CloudTrail: Used to log actions taken by users and services within our AWS account.
- AWS GuardDuty: Used for intrusion and threat detection within our AWS account.
- Postgres Logs: Used for detecting issues with our production Postgres database.
- AWS Inspector: Used for detecting vulnerabilities on our production EC2 hosts.
- Okta Logs: Used to log actions done by our users within Okta.
- Sentry: Used to aggregate errors that occur within our application.

CodeSee is constantly striving to improve our security monitoring capabilities and uses AWS' documentation on best practices to inform the alarming and logging measures we take.

Incident Management

CodeSee's incident response procedures are detailed in its Security Incident Response Plan. Our primary goals will be to investigate, contain any exploitations, eradicate any threats, recover CodeSee systems, and remediate any vulnerabilities. Throughout this process, thorough documentation will be required as well as a post-mortem report.
Specific steps that CodeSee will take are:

- The Security Manager will manage the incident response effort.
- All correspondence will take place within the "War Room" CodeSee Slack channel.
- A recurring Incident Response Meeting will be held at regular intervals until the incident is resolved.
- CodeSee will inform all necessary parties of the incident without undue delay.

Data Backup and Recovery

CodeSee uses redundant RDS instances to ensure quick failover in the event of an outage. CodeSee also maintains daily snapshot backups that are retained for 7 days. For local files of employee workstations, CodeSee has a shared google drive which acts as a backup.

System Account Management

CodeSee's access management procedures are documented in its Access Control Policy. The following requirements are in place with respect to access control:

- **Principle of Least Privilege** - Users of CodeSee systems will be given minimum access to data and systems based on job function, business requirements, or need-to-know for that specific user.
- **Unique Accounts** - Users of CodeSee systems and applications will be provided with unique credentials (IDs, keys, etc.) that can be used to trace activities to the individual responsible for that account.
- **Password Security** - Unique accounts and passwords are required for all users. The following also applies for all passwords:
    - **Rotation Requirements** - If a password is suspected to be compromised, the password should be rotated immediately and the security team should be immediately notified.

- **Storing Passwords** - Passwords must only be stored using a CodeSee approved password manager.
- **Multi-Factor Authentication** - When available, multi-factor authentication should be used.

In order to onboard new personnel, the following steps should be taken and documented:

1. Any CodeSee devices provided to the new hire must be inventoried in accordance with CodeSee Policy.
2. A new hire email or ticket is sent to the appropriate team to inform them of new personnel.
3. IT/Engineering and the new personnel's manager document a checklist of accounts and permission levels needed for that hire.
4. The applicable team sets up each user with the appropriate access.
5. All of the onboarding processes should be appropriately documented via ticketing or other document management tools.

Risk Management Program

Data Classification

CodeSee has four classifications for the data it uses, processes, and produces. The classifications are:

- **Public**
- **Internal**
- **Confidential**
- **Restricted**

Public data is information that may be disclosed to any person regardless of their affiliation with CodeSee. The Public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that does not require any level of protection from disclosure. While it may be necessary to protect original (source) documents from unauthorized modification, Public data may be shared with a broad audience both within and outside CodeSee and no steps need be taken to prevent its distribution. Public data can be retained for an indefinite period of time.

Examples of Public data include:

- Published press releases;
- Published documentation
- Published blog posts
- Anything on the CodeSee public website
- Anything on CodeSee social media profiles

Internal data is information that is potentially sensitive and is not intended to be shared with the public. Internal data should be classified as such when the unauthorized disclosure, alteration, or destruction of that data would result in a moderate risk to CodeSee, its customers, or its partners. Internal data generally should not be disclosed outside of CodeSee without the permission of the person

or group that created the data. It is the responsibility of the data owner to designate information as Internal where appropriate. If you have questions about whether the information is Internal or how to treat Internal data, you should talk to your manager or send an email to shanea@codesee.io. Internal data can be retained for an indefinite period of time.

Examples of Internal data include:

-
- Unpublished CodeSee memos
- Unpublished marketing materials
- Non-public CodeSee customer and partner names
- Procedural documentation that should remain private

Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals or CodeSee. This classification also includes data that CodeSee may be required to keep confidential, either by law or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported. Confidential data should be retained only as long as it is needed to conduct internal/external business operations. Customer deletion requests and contractual deletion obligations should be the main source of authority for storing/deleting Confidential data, as applicable.

Examples of Confidential data include:

- Individual employment information, including salary, benefits and performance evaluations for current, former, and prospective employees
- Legal documents
- Customer data
- Contractual agreements
- Compliance reports such as SOC 2
- Data that is subject to an NDA or other confidentiality clause
- Information shared by partners or investors

Restricted data includes any information that CodeSee has a legal or regulatory obligation to safeguard in the most stringent manner. Data should be classified as Restricted when the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to CodeSee, its customers, or its partners. The highest level of security controls should be applied to Restricted data.

Examples of Restricted data include:

- CodeSee codebase
- Intellectual property
- Passwords, private keys, and other credentials
- Bank information
- Tax IDs
- Information related to pending litigation or investigations
- Data required to be protected by regulatory obligations

- Additional employment information such as background checks, health, and medical information, social security numbers.

Risk Management Responsibilities

Role	Responsibility
CEO	Ultimately responsible party for the acceptance and/or treatment of any risks to the organization.
CTO	Can approve the avoidance, remediation, transference, or acceptance of any risk cited in the Risk Register. This person shall be responsible for communicating risks to top management and the board and adopting risk treatments in accordance with the executive direction.
IT Manager	Shall be responsible for adherence to the Risk Management Policy.

Additional details related to risk management are in CodeSee's Risk Assessment and Treatment Policy.

Risk Management Program Activities

On a practical level, CodeSee's Risk Management process involves **3 stages**:

- Identification of risks,
- Assessment of their potential impact, and
- CodeSee's risk treatment towards the risk.

Identification of risks involves categorization and investigation. Examples of categories used are

- **Technical,**
- **Reputational,**
- **Contractual,**
- **Financial,**
- **Regulatory, and**
- **Fraud risks**.

CodeSee's Business Continuity and Disaster Recovery Plan detail our key business processes and critical services.

Risk Assessment

CodeSee's Risk Assessment process takes into account a number of factors each of which contributes to both the likelihood and potential impact of a given risk. These include:

- The criticality of potentially impacted business processes as laid out in the Business Continuity and Disaster Recovery Policy.
- Whether a risk could potentially impact the confidentiality, availability, integrity, or privacy of customer data, or PII.
- Potential monetary loss.
- The ability of the risk to impact CodeSee's business objectives.
- Potential impact to CodeSee customers or vendors

CodeSee uses Risk Treatment Plans for any response to risks other than "Accept."

Risk Analysis

CodeSees Risk Analysis Method is as follows:

	RISK =LIKELIHOOD *IMPACT	LIKELIHOOD				
		Very high: 5	High: 4	Moderate 3	Low 2	Very Low 1
IMPACT	Very High: 5	25	20	15	10	5
	High: 4	20	16	12	8	4
	Moderate: 3	15	12	9	6	3
	Low: 2	10	8	6	4	2
	Very low: 1	5	4	3	2	1

RISK LEVEL	RISK DESCRIPTION
Low (1-6)	A threat event could be expected to have a limited adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.
Moderat (7-19)	A threat event could be expected to have a serious adverse effect on organizational operations, mission capabilities, assets, individuals, customers, or other organizations
High (20-25)	A threat event could be expected to have a severe adverse effect on organizational operations, mission capabilities, assets, individuals, customers, or other organizations.

IMPACT LEVEL	IMPACT DESCRIPTION

Very Low / Low	A threat event could be expected to have a limited adverse effect, meaning: degradation of mission capability yet primary functions can still be performed; minor damage; minor financial loss; or range of effects is limited to some cyber resources but no critical resources.
Moderate	A threat event could be expected to have a serious adverse effect, meaning: significant degradation of mission capability yet primary functions can still be performed at a reduced capacity; minor damage; minor financial loss; or range of effects is significant to some cyber resources and some critical resources.
High / Very High	A threat event could be expected to have a severe or catastrophic adverse effect, meaning: severe degradation or loss of mission capability and one or more primary functions cannot be performed; major damage; major financial loss; or range of effects is extensive to most cyber resources and most critical resources.

LIKELIHOOD LEVEL	LIKELIHOOD DESCRIPTION
Very Low / Low	Adversary is unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is unlikely to occur; or threat is unlikely to have adverse impacts.
Moderate	Adversary is somewhat unlikely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is somewhat unlikely to occur; or threat is somewhat unlikely to have adverse impacts.
High / Very High	Adversary is highly likely to initiate a threat event; non-adversarial threat event (e.g., nature, error, accident) is highly likely to occur; or threat is highly likely to have adverse impacts.

Risk Response

In accordance with CodeSee's Risk Assessment and Treatment Policy, risks will be prioritized and mapped according to the descriptions listed above. The following responses to risk should be employed. Where CodeSee chooses a risk response other than "Accept," it shall develop a Risk Treatment Plan.

- Mitigate: CodeSee may take actions or employ strategies to reduce the risk.
- Accept: CodeSee may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events.
- Transfer: CodeSee may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by CodeSee, or insurance may be appropriate for protection against financial loss.
- Eliminate: The risk may be such that CodeSee could decide to cease the activity or to change it in such a way as to end the risk.

Integration with Risk Assessment

CodeSee is committed to handling and remediating risks inherent in any commitments, agreements, or responsibilities it may enter into or take on during the operation of the company. Due to the nature of these risks, it may be necessary for CodeSee to develop specialized controls. CodeSee takes into account all relevant factors; contractual, legal, and regulatory when designing these controls. CodeSee's CTO has the final say on the design and implementation of these controls.
In general, CodeSee's Risk Assessment procedure is still applicable to risks inherent in CodeSee's commitments and contractual responsibilities and should be applied to determining the severity of risks.

Information and Communications Systems

CodeSee uses Slack for restricted internal communications. CodeSee also uses Zoom and a company Gmail for both internal and external communications.

For workflow, project management, and sharing of internal documents CodeSee uses Jira and Coda as well as a company Google Drive.

Data Communication

CodeSee uses HTTPS to communicate with and access its network, along with public-facing bastion servers are used to control SSH traffic to and from the network. IP addresses have to be specifically whitelisted to allow access and implicit denial is employed. All traffic to the network is redirected from HTTP to HTTPS.

Access Control to the production codebase is limited via the following controls:

- 2FA-protected accounts must be used to access any part of CodeSee's codebase
- The production code branch is protected, requiring a merge request and approval before any changes can be made. This also protects the branch from being deleted.
- RBAC approach is used for accessing the application code repository.
- All default regular-user accounts have been removed.

Monitoring Controls

CodeSee takes a dual approach to continuous monitoring using both internal monitoring and relying on third parties.

Internal Monitoring

CodeSee has a highly interconnected business process allowing for visibility and insight by management into the operations of each department. Corrective action is initiated through direct zoom calls. Within departments, code reviews and automated testing help ensure internal controls are being followed and implemented.

Third-Party Monitoring

CodeSee contracts a third party to perform annual penetration tests and uses vulnerability scanners (e.g. AWS Inspector, Snyk) to monitor for new vulnerabilities. The vulnerability scanners are also used for tracking and logging known vulnerabilities.

The process for reporting any deficiencies with regards to CodeSee policies and procedures is clearly spelled out in each relevant Policy.

DC 6: Complementary User Entity Controls (CUECs)

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

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

- User entities are responsible for understanding and complying with their contractual obligations to CodeSee.
- User entities are responsible for notifying CodeSee of changes made to technical or administrative contact information.
- User entities are responsible for maintaining their own system(s) of record.
- User entities are responsible for ensuring the supervision, management, and control of the use of CodeSee services by their personnel.
- User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize CodeSee services.

- User entities are responsible for immediately notifying CodeSee of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
- The user entity controls presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities are responsible for the following:

Trust Services Criteria	Complementary User Entity Controls
CC2.1	User entities are responsible for the security and integrity of data housed under user entity control, particularly the data utilized by CodeSee 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 CodeSee's application keys and API keys for access to the webservice 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 CodeSee.
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 CodeSee.
C1.1	User entities assign responsibility to personnel, and those personnel identify which data used by CodeSee is to be considered "sensitive".

DC 7: Complementary Subservices Organization Controls (CSOCs)

AWS

CodeSee uses AWS as a subservice organization for data center colocation services. CodeSee's controls related to their system cover only a portion of the overall internal control for each user entity of the System. The description does not extend to the services provided by the subservice organization that provides colocation services for IT infrastructure. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of AWS.

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 CodeSee receives and reviews the AWS SOC 2 report annually. In addition, through its operational activities, CodeSee 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 CodeSee. Therefore, each user entity's internal control must be evaluated in conjunction with CodeSee's controls and related tests, and results described in Section 4 of this report, considering the related CSOCs expected to be implemented at the subservice organization as described below.

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

Okta

CodeSee uses Okta as a subservice organization to provide identity and access management (IAM). CodeSee's controls related to their system cover only a portion of the overall internal control for each user entity of the System. The description does not extend to the services provided by the subservice organization that provides IAM services. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of Okta.

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 Okta related to logical access controls, system operations, change management, and risk mitigation related to availability.

Management of CodeSee receives and reviews the Okta SOC 2 report annually. In addition, through its operational activities, CodeSee management monitors the services performed by Okta 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 Okta management.

It is not feasible for the criteria related to the System to be achieved solely by CodeSee. Therefore, each user entity's internal control must be evaluated in conjunction with CodeSee'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
CC6.1	Okta is responsible for: • Managing Identification and Authentication • Managing Credentials for Infrastructure and Software • Using Encryption to Protect Data • Protecting Encryption Keys
CC6.2	Okta is responsible for: • controlling Access Credentials to Protected Assets
CC6.3	Okta is responsible for: • implementing Role-Based Access Controls • removing access to Protected Information Assets • creating or modifying Access to Protected Information Assets
CC6.6	Okta is responsible for:

	• protecting Identification and Authentication Credentials
CC6.7	Okta uses encryption technologies or secure communications channels to protect data
CC7.2	Okta is responsible for monitoring system components and the operation of those components for anomalies that are indicative of malicious acts
CC7.3	Okta is responsible for evaluating security events to identify security failures, and taking actions to prevent or address failures
CC7.4	Okta is responsible for responding to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	Okta is responsible for identifying, developing, and implementing activities to recover from identified security incidents.
CC8.1	Okta is responsible for authorizing, designing, developing, configuring, documenting, testing, approving, and implementing changes to infrastructure, data, software, and procedures.
CC9.1	Okta is responsible for identifying, and developing risk mitigation activities for risks arising from potential business disruptions.

DC 8: Any specific criterion of the applicable trust services criteria that is not relevant to the system and the reasons it is not relevant

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.

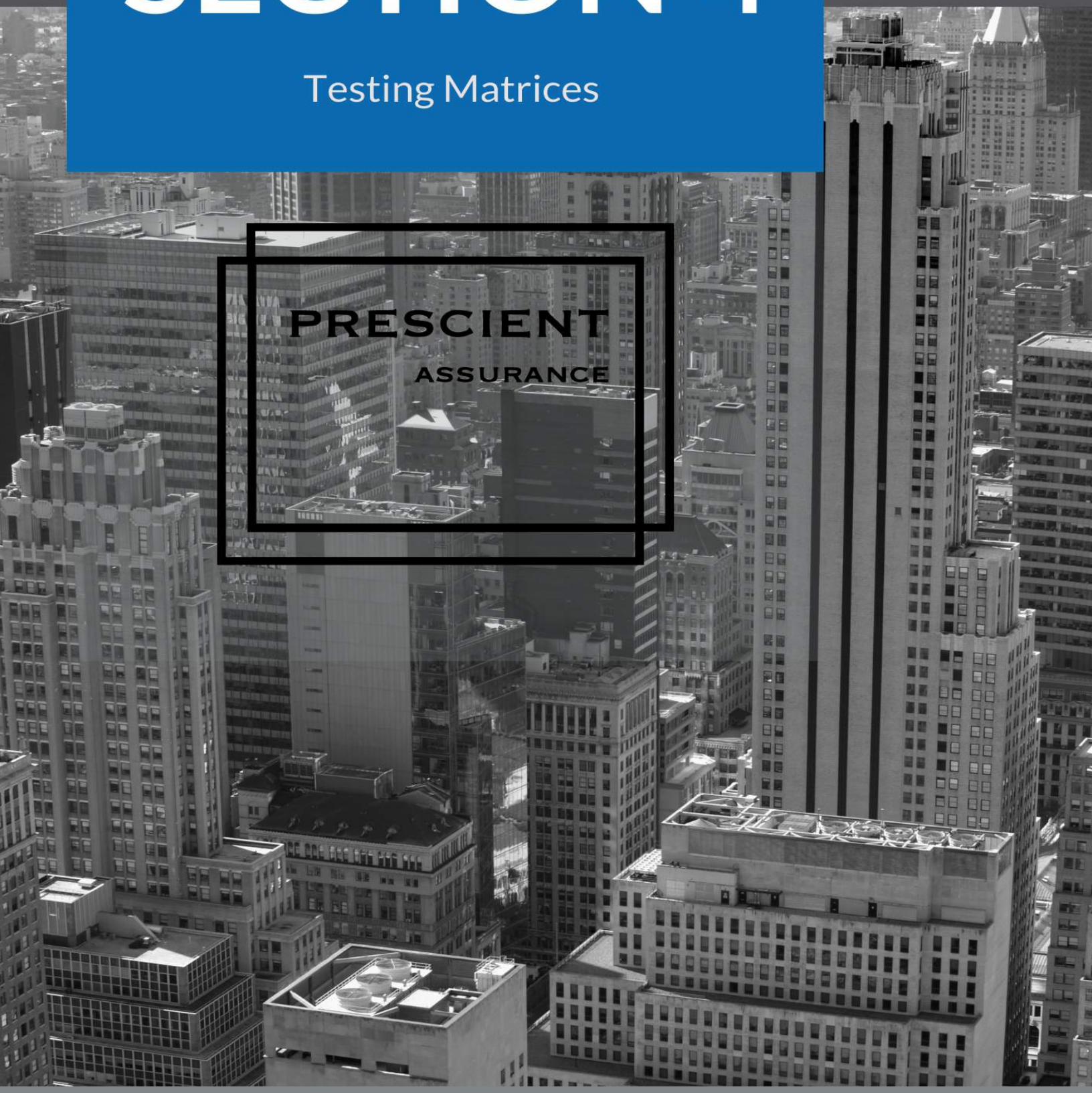
This criterion does not apply to CodeSee because we do not have any physical facilities requiring restricted physical access.

DC 9: Disclosure of Significant changes in last 1 year

The system did not exist 1 year ago. One year ago, the company personnel consisted of Shanea Leven, Joshua Leven, and Daniel (cubes) Silverstein. Everyone else has been hired in the last year.

SECTION 4

Testing Matrices



Tests of Operating Effectiveness and Results of Tests

Scope of Testing

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

Prescient Assurance LLC conducted the examination testing throughout the period November 18, 2021, to February 18, 2022

The tests applied to test the Operating Effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonably, 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 the 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 the existence of initials or signatures. • Examination / Inspection of systems documentation, configurations, and settings; and • Examination / Inspection of procedural documentation such as operations manuals, flow charts, and job descriptions.

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

General Sampling Methodology

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Prescient Assurance utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, to determine the number of items to be selected in a sample for a particular test.

Prescient Assurance, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

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

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

Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, many times per day	At least 25	**At least 40**
Manual control, daily (Note 1)	At least 25	**At least 40**
Manual control, weekly	At least 5	**At least 10**
Manual control, monthly	At least 3	**At least 4**
Manual control, quarterly	At least 2	**At least 2**

Manual control, annually	Test annually	**Test annually**
Application controls	Test one operation of each relevant aspect of each application control if supported by effective IT general controls; otherwise test at least 15	**Test one operation of each application control if supported by effective IT general controls; otherwise test at least 25**
IT general controls	Follow guidance above for manual and automated aspects of IT general controls	**Follow guidance above for manual and automated aspects of IT general controls**

Notes: 1.) Some controls might be performed frequently, but less than daily. For such controls, the sample size should be interpolated using the above guidance. Generally, for controls where the number of occurrences ranges from 50 to 250 during the year, our minimum sample size using the above table should be approximately 10% of the number of occurrences.

Reliability of Information Provided by the Service Organization

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

Test Results

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

Any phrase other than the above constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the Operating Effectiveness of the control activity.

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

Trust ID	Standard Description	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.	Observed background check data on Secureframe to find that 11 of 11 eligible employees have completed background checks documented. A 12th employee started at CodeSee in February 2022 and is still within the SLA of completing onboarding procedures as of this audit.	No exceptions noted.
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Observed a Signed Contractual Agreement to determine contractors agree to the code of conduct and company policies at the time of engagement. Sampled 4 of 4 Contractor Agreements to determine contractors acknowledge company policies including the code of conduct.	No exceptions noted.
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Observed Secureframe to find 11 of 11 eligible employees have agreed to the Code of Conduct. Inspected the Code of Conduct to determine there are enforcement procedures documented that include disciplinary action. A 12th employee started at CodeSee in February 2022 and is still within the SLA of completing onboarding procedures as of this audit.	No exceptions noted.
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Observed a sample of 5 Confidentiality Agreements to determine contractors are required to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to sign a confidentiality agreement during onboarding.	Observed a sample of 5 Confidentiality Agreements to determine employees are required to sign a confidentiality agreement at the time of hire.	No exceptions noted.
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company managers are required to complete performance evaluations for direct reports at least annually.	Observed a Performance Evaluation to determine there are performance measures established and sampled 5 of 12 employee performance evaluations to determine they are completed. Inspected the Performance Review Policy to determine performance reviews are conducted annually.	No exceptions noted.

CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	Inspected the Board Meeting Minutes to observe the organization's welfare was discussed.	No exceptions noted.
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the Bylaws to observe the roles and responsibilities of the board of directors are documented.	No exceptions noted.
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.	Sampled 2 of 3 Board Member Linkedin Profiles to determine board members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls.	No exceptions noted.
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	Inspected 2 Board Meeting Minutes to observe board meetings are conducted at least biannually, formal meeting minutes are kept, and independent directors attended the meeting.	No exceptions noted.
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the Bylaws to observe the roles and responsibilities of the board of directors are documented.	No exceptions noted.
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and	The company management has established defined roles and responsibilities to oversee the design and implementation of	Inspected a Product Manager Job Description to observe the responsibilities of management and to determine management is responsible for the oversight of the	No exceptions noted.

	responsibilities in the pursuit of objectives.	information security controls.	design and implementation of information security controls.	
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected an Organization Chart to observe the organizational structure and established reporting lines.	No exceptions noted.
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected an Executive Assistant / Operations Lead Job Description to determine responsibilities for the design, implementation, operation, maintenance, and monitoring of information security controls are assigned within job descriptions.	No exceptions noted.
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company performs background checks on new employees.	Observed background check data on Secureframe to find that 11 of 11 eligible employees have completed background checks documented. A 12th employee started at CodeSee and is still within the SLA of completing onboarding procedures as of this audit.	No exceptions noted.
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Observed a Performance Evaluation to determine there are performance measures established and sampled 5 of 12 employee performance evaluations to determine they are completed. Inspected the Performance Review Policy to determine performance reviews are conducted annually.	No exceptions noted.
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected an Executive Assistant / Operations Lead Job Description to determine responsibilities for the design, implementation, operation, maintenance, and monitoring of information security controls are assigned within job descriptions.	No exceptions noted.
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain	The company requires employees to complete security awareness training within thirty days of hire	Observed Secureframe to determine security training is conducted. 11 of 11 eligible employees have completed	No exceptions noted.

	competent individuals in alignment with objectives.	and at least annually thereafter.	security training. Inspected the Information Security Policy to determine employees are required to complete security training at the time of hire and annually thereafter. A 12th employee started at CodeSee in February 2022 and is still within the SLA of completing onboarding procedures as of this audit.	
CC 1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Observed Secureframe to determine 11 of 11 eligible employees have agreed to the code of conduct. Inspected the Code of Conduct to determine there are enforcement procedures documented that include disciplinary action. A 12th employee started at CodeSee in February 2022 and is still within the SLA of completing onboarding procedures as of this audit.	No exceptions noted.
CC 1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Observed a Performance Evaluation to determine there are performance measures established and sampled 5 of 12 employee performance evaluations to determine they are completed. Inspected the Performance Review Policy to determine performance reviews are conducted annually.	No exceptions noted.
CC 1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected an Executive Assistant / Operations Lead Job Description to determine responsibilities for the design, implementation, operation, maintenance, and monitoring of information security controls are assigned within job descriptions.	No exceptions noted.
CC 2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Observed Secureframe to determine all relevant policies have been published and have been reviewed within the last year. Inspected the Information Security Policy to determine security policies are reviewed and updated at least annually to verify controls are operating effectively.	No exceptions noted.
CC 2.1	COSO Principle 13: The entity obtains or	The company utilizes a log management tool to identify	Observed a screenshot of log evidence to determine that event	No exceptions noted.

	generates and uses relevant, quality information to support the functioning of internal control.	events that may have a potential impact on the company's ability to achieve its security objectives.	logs are maintained to assist with the achievement of security objectives.	
CC 2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Observed Secureframe to determine that there are vulnerability scans conducted, that findings are given severity ratings, and that they are tracked to remediation.	No exceptions noted.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Policy to determine there are privacy and incident response processes and procedures documented and communicated to all necessary personnel.	No exceptions noted.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected a Product Manager Job Description to observe the responsibilities of management and to determine management is responsible for the oversight of the design and implementation of information security controls.	No exceptions noted.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected an Executive Assistant / Operations Lead Job Description to determine responsibilities for the design, implementation, operation, maintenance, and monitoring of information security controls are assigned within job descriptions.	No exceptions noted.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Observed Secureframe to determine security training is conducted. 11 of 11 eligible employees have completed security training. Inspected the Information Security Policy to determine employees are required to complete security training at the time of hire and annually thereafter. A 12th employee	No exceptions noted.

			started at CodeSee in February 2022 and is still within the SLA of completing onboarding procedures as of this audit.	
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company's information security policies and procedures are documented and reviewed at least annually.	Observed Secureframe to determine all relevant policies have been published and have been reviewed within the last year. Inspected the Information Security Policy to determine security policies are reviewed and updated at least annually.	No exceptions noted.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Observed the CodeSee Website to determine there is a description of their product communicated to internal and external users.	No exceptions noted.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company communicates system changes to authorized intern al users.	Observed a Screenshot of a GitHub communication chane to determine system changes are communicated to authorized internal users.	No exceptions noted.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Observed a Screenshot of an Anonymous Communication Form to determine there is an Anonymous communication channel in place that allows users to anonymously report issues and or fraud concerns.	No exceptions noted.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Observed the CodeSee Website to determine there is a publicly available terms of service that communicates commitments.	No exceptions noted.
CC 2.3	COSO Principle 15: The entity communicates	The company notifies customers of critical system	Observed the CodeSee Website to determine there is a publicly	No exceptions noted.

	with external parties regarding matters affecting the functioning of internal control.	changes that may affect their processing.	available changelog where system changes that may affect user processing are communicated.	
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides guidelines and technical support resources relating to system operations to customers.	Observed the CodeSee Website to determine there are publicly available technical support resources that relate to system operations that include demo, blog, maps docs, recordings docs, changelog, and press.	No exceptions noted.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Observed the CodeSee Website to determine there is a description of their product communicated to internal and external users.	No exceptions noted.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Observed the CodeSee Website to determine there is a publicly available support email established where users are able to report system failures, incidents, concerns, and or other complaints to appropriate personnel.	No exceptions noted.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Observed a sample Signed Non Disclosure Agreement to determine there are confidentiality and privacy agreements made with contractors and third-parties.	No exceptions noted.
CC 3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Assessment and Treatment Policy to determine there are risk categories documented to help with the identification and assessment of risk related to objectives.	No exceptions noted.
CC 3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Assessment and Treatment Policy to determine the risk management processes and procedures of scoping assets, identification of threats and vulnerabilities, analysis of risk, risk treatment, calculation of residual risk, and reporting are documented. Observed Secureframe to determine there is a risk registry maintained with identified vulnerabilities,	No exceptions noted.

			vulnerabilities are given severity ratings, and vulnerabilities are tracked to remediation.	
CC 3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Observed a Business Continuity and Disaster Recovery Tabletop Exercise to determine the business continuity and disaster recovery plan is tested. Inspected the Business Continuity and Disaster Recovery Plan to determine the plan is tested at least annually.	No exceptions noted.
CC 3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Observed Secureframe to determine there are risk assessments conducted, risks are identified and remediated, and a risk registry is maintained. Inspected the System Description to determine fraud is considered during the risk assessment process. Inspected the Risk Assessment and Treatment Policy to determine risk assessments are conducted annually or whenever there are significant changes.	No exceptions noted.
CC 3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Assessment and Treatment Policy to determine the risk management processes and procedures of scoping assets, identification of threats and vulnerabilities, analysis of risk, risk treatment, calculation of residual risk, and reporting are documented. Observed Secureframe to determine there is a risk registry maintained with identified vulnerabilities, vulnerabilities are given severity ratings, and vulnerabilities are tracked to remediation.	No exceptions noted.
CC 3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Observed Secureframe to determine there is a vendor list maintained where vendors are given severity ratings, hve security and privacy requirements, and have reviews conducted periodically. Inspected the Vendor Management Policy to determine there are contract reviews that review contractor privacy and security commitments., annual	No exceptions noted.

			vendor reviews, risk assessment, and due diligence procedures documented.	
CC 3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Observed Secureframe to determine there are risk assessments conducted, risks are identified and remediated, and a risk registry is maintained. Inspected the System Description to determine fraud is considered during the risk assessment process. Inspected the Risk Assessment and Treatment Policy to determine risk assessments are conducted annually or whenever there are significant changes.	No exceptions noted.
CC 3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Assessment and Treatment Policy to determine the risk management processes and procedures of scoping assets, identification of threats and vulnerabilities, analysis of risk, risk treatment, calculation of residual risk, and reporting are documented. Observed Secureframe to determine there is a risk registry maintained with identified vulnerabilities, vulnerabilities are given severity ratings, and vulnerabilities are tracked to remediation.	No exceptions noted.
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Observed a Screenshot of GitHub to determine GitHub is used to manage configurations and verify configurations are deployed consistently throughout the environment.	No exceptions noted.
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Observed a Penetration Test Report to determine there are penetration tests conducted and identified vulnerabilities are tracked to remediation. Inspected the Vulnerability and Patch Management Policy to determine there are third-party penetration tests conducted at least annually.	No exceptions noted.
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that	The company's risk assessments are performed at least annually. As part of	Observed Secureframe to determine there are risk assessments conducted, risks are	No exceptions noted.

	could significantly impact the system of internal control.	this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	identified and remediated, and a risk registry is maintained. Inspected the System Description to determine fraud is considered during the risk assessment process. Inspected the Risk Assessment and Treatment Policy to determine risk assessments are conducted annually or whenever there are significant changes.	
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Assessment and Treatment Policy to determine the risk management processes and procedures of scoping assets, identification of threats and vulnerabilities, analysis of risk, risk treatment, calculation of residual risk, and reporting are documented. Observed Secureframe to determine there is a risk registry maintained with identified vulnerabilities, vulnerabilities are given severity ratings, and vulnerabilities are tracked to remediation.	No exceptions noted.
CC 4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Observed Secureframe to determine all relevant policies have been published and have been reviewed within the last year. Inspected the Information Security Policy to determine security policies are reviewed and updated at least annually to verify controls are operating effectively.	No exceptions noted.
CC 4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Observed a Penetration Test Report to determine there are penetration tests conducted and identified vulnerabilities are tracked to remediation. Inspected the Vulnerability and Patch Management Policy to determine there are third-party penetration tests conducted at least annually.	No exceptions noted.
CC 4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and	Observed Secureframe to determine there is a vendor list maintained where vendors are given severity ratings, hve security and privacy requirements, and have reviews conducted periodically. Inspected the Vendor	No exceptions noted.

	of internal control are present and functioning.	privacy requirements; and - review of critical third-party vendors at least annually.	Management Policy to determine there are contract reviews that review contractor privacy and security commitments., annual vendor reviews, risk assessment, and due diligence procedures documented.	
CC 4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. critical and high vulnerabilities are tracked to remediation.	Observed Secureframe to determine that there are vulnerability scans conducted, that findings are given severity ratings, and that they are tracked to remediation.	No exceptions noted.
CC 4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Observed Secureframe to determine all relevant policies have been published and have been reviewed within the last year. Inspected the Information Security Policy to determine security policies are reviewed and updated at least annually to verify controls are operating effectively.	No exceptions noted.
CC 4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Observed Secureframe to determine there is a vendor list maintained where vendors are given severity ratings, hve security and privacy requirements, and have reviews conducted periodically. Inspected the Vendor Management Policy to determine there are contract reviews that review contractor privacy and security commitments., annual vendor reviews, risk assessment, and due diligence procedures documented.	No exceptions noted.
CC 5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Assessment and Treatment Policy to determine the risk management processes and procedures of scoping assets, identification of threats and vulnerabilities, analysis of risk, risk treatment, calculation of residual risk, and reporting are documented. Observed Secureframe to determine there is a risk registry maintained with identified vulnerabilities,	No exceptions noted.

			vulnerabilities are given severity ratings, and vulnerabilities are tracked to remediation.	
CC 5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company's information security policies and procedures are documented and reviewed at least annually.	Observed Secureframe to determine all relevant policies have been published and have been reviewed within the last year. Inspected the Information Security Policy to determine security policies are reviewed and updated at least annually.	No exceptions noted.
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control and Termination Policy to determine there are onboarding, modifying, and offboarding procedures documented. Observed 2 Quarterly Access Reviews to determine access provisioning, modifying, and removal procedures are followed.	No exceptions noted.
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine there are processes and procedures for the development, engineering, security, checking, testing, implementing, version control, change control, and test data documented. Observed a Screenshot of GitHub to determine the SDLC is followed.	No exceptions noted.
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's information security policies and procedures are documented and reviewed at least annually.	Observed Secureframe to determine all relevant policies have been published and have been reviewed within the last year. Inspected the Information Security Policy to determine security policies are reviewed and updated at least annually.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the Change Management Policy to determine the steps taken for software and infrastructure changes: product roadmap, planning, evaluating, building, testing, documenting, code reviewing, approval, implementing, communication, and post change review. Observed a Screenshot of changes on GitHub to determine changes are approved and that the change management process is followed.	No exceptions noted.

CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's data backup policy documents requirements for backup and recovery of customer data.	Observed the Business Continuity and Disaster Recovery Tabletop Exercise to determine the backup processes are tested. Inspected the Information Security Policy to determine there are backup processes and procedures documenting that backups should be conducted according to appropriate schedules and that necessary systems, datta, and configurations can be recovered in the event of a disaster.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Retention and Disposal Policy to determine there are data retention and disposal processes and procedures documented to assist with the secure retention or disposal of data and customer data is deleted within 30 days of request. Observed Secureframe to determine there is a disposal log used to assist with the secure disposal of company and customer data.	Disclosure there was no data disposed of during the audit window.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine there are processes and procedures for the development, engineering, security, checking, testing, implementing, version control, change control, and test data documented. Observed a Screenshot of GitHub to determine the SDLC is followed.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Policy to determine there are privacy and incident response processes and procedures documented and communicated to all necessary personnel.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Assessment and Treatment Policy to determine there are risk categories documented to help with the identification and assessment of risk related to objectives.	No exceptions noted.

CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Assessment and Treatment Policy to determine the risk management processes and procedures of scoping assets, identification of threats and vulnerabilities, analysis of risk, risk treatment, calculation of residual risk, and reporting are documented. Observed Secureframe to determine there is a risk registry maintained with identified vulnerabilities, vulnerabilities are given severity ratings, and vulnerabilities are tracked to remediation.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and responsibilities policy.	Inspected an Executive Assistant / Operations Lead Job Description to determine responsibilities for the design, implementation, operation, maintenance, and monitoring of information security controls are assigned within job descriptions.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's information security policies and procedures are documented and reviewed at least annually.	Observed Secureframe to determine all relevant policies have been published and have been reviewed within the last year. Inspected the Information Security Policy to determine security policies are reviewed and updated at least annually.	No exceptions noted.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Observed Secureframe to determine there is a vendor list maintained where vendors are given severity ratings, hve security and privacy requirements, and have reviews conducted periodically. Inspected the Vendor Management Policy to determine there are contract reviews that review contractor privacy and security commitments., annual vendor reviews, risk assessment, and due diligence procedures documented.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information	The company restricts privileged access to the application to authorized users with a business need.	Observed a Quarterly Access Review to determine access is reviewed and adjusted based on business need. Inspected the Access Control and Termination	No exceptions noted.

	assets to protect them from security events to meet the entity's objectives.		Policy to determine the principle of least privilege is followed and access is restricted based on business need.	
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control and Termination Policy to determine there are onboarding, modifying, and offboarding procedures documented. Observed 2 Quarterly Access Reviews to determine access provisioning, modifying, and removal procedures are followed.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to databases to authorized users with a business need.	Observed a Quarterly Access Review to determine access is reviewed and adjusted based on business need. Inspected the Access Control and Termination Policy to determine the principle of least privilege is followed and access to databases is restricted based on business need.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH keys.	Observed a Screenshot of 1Password to determine users have unique authentication IDs. Inspected the Access Control and Termination Policy to determine users are required to have unique authorized authentication.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to encryption keys to authorized users with a business need.	Observed a Quarterly Access Review to determine access is reviewed and adjusted based on business need. Inspected the Access Control and Termination Policy to determine the principle of least privilege is followed and access is restricted based on business need.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the firewall to authorized users with a business need.	Observed a Quarterly Access Review to determine access is reviewed and adjusted based on business need. Inspected the Access Control and Termination Policy to determine the principle of least privilege is followed and access to systems is restricted based on business need.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure,	The company restricts privileged access to the operating system to	Observed a Quarterly Access Review to determine access is reviewed and adjusted based on	No exceptions noted.

	and architectures over protected information assets to protect them from security events to meet the entity's objectives.	authorized users with a business need.	business need. Inspected the Access Control and Termination Policy to determine the principle of least privilege is followed and access to the production servers is restricted based on business need.	
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the production network to authorized users with a business need.	Observed a Quarterly Access Review to determine access is reviewed and adjusted based on business need. Inspected the Access Control and Termination Policy to determine the principle of least privilege is followed and access to production servers is restricted based on business need.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Observed a New Account Checklist to determine access is granted based on job role Inspected the Access Control and Termination Policy to determine the principle of least privilege is followed and access is modified based on job need and must be approved.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Observed a Screenshot of 1Password to determine users have unique authentication IDs. Inspected the Access Control and Termination Policy to determine users are required to have unique authorized authentication.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts access to migrate changes to production to authorized personnel.	Observed a Quarterly Access Review to determine access is reviewed and adjusted based on business need. Inspected the Access Control and Termination Policy to determine the principle of least privilege is followed and access is restricted based on business need.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the System Description to determine there are data handling procedures documented to help identify and organize different data types. Inspected the Data Classification Policy to determine there are confidential data handling, securing and restricting procedures documented.	No exceptions noted.

CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's datastores housing sensitive customer data are encrypted at rest.	Observed a CloudTrail Report to determine datastores storing customer data are encrypted at rest.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's network is segmented to prevent unauthorized access to customer data.	Observed a Screenshot of a Dashboard of Segmented Environments to determine the network is segmented to prevent unauthorized access to customer data.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires passwords for in-scope system components to be configured according to the company's policy.	Observed a Screenshot of 1Password to determine users have unique IDs. Inspect the System Description to determine there are password rotation, storing, and multi-factor authentication procedures documented. Inspected the Information Security Policy to determine users are required to have unique passwords and passwords must be a minimum of 8 characters containing at least one uppercase letter, lowercase letter, a number, and a special character.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company maintains a formal inventory of production system assets.	Observed Secureframe to determine there is an inventory of assets maintained.	No exceptions noted.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Observed a Screenshot of CloudFlare to determine authorized personnel are required to have and use MFA when accessing the production systems.	No exceptions noted.
CC 6.1	The entity implements logical access security	The company's production systems can only be	Observed the CodeSee Website to determine there is a valid web	No exceptions noted.

	software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	remotely accessed by authorized employees via an approved encrypted connection.	certificate in place and the connection is secured with SSL.	
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Observed a Screenshot of 1Password to determine users have unique authentication IDs. Inspected the Access Control and Termination Policy to determine users are required to have unique authorized authentication.	No exceptions noted.
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control and Termination Policy to determine there are onboarding, modifying, and offboarding procedures documented. Observed 2 Quarterly Access Reviews to determine access provisioning, modifying, and removal procedures are followed.	No exceptions noted.
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Observed a Quarterly Access Review to determine there are access reviews conducted, access is modified based on business need, and sampled 2 of 2 access reviews to determine they are conducted quarterly. Inspected the Access Control and Termination Policy to determine access is restricted based on the principle of least privilege and changes are required to be approved and documented.	No exceptions noted.
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Observed a Screenshot of an Employee's Access Removal Procedures to determine there is a termination checklist followed and access is appropriately removed upon termination.	No exceptions noted.

	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.			
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Observed a New Account Checklist to determine access is granted based on job role Inspected the Access Control and Termination Policy to determine the principle of least privilege is followed and access is modified based on job need and must be approved.	No exceptions noted.
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Observed a Screenshot of 1Password to determine users have unique authentication IDs. Inspected the Access Control and Termination Policy to determine users are required to have unique authorized authentication.	No exceptions noted.
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control and Termination Policy to determine there are onboarding, modifying, and offboarding procedures documented. Observed 2 Quarterly Access Reviews to determine access provisioning, modifying, and removal procedures are followed.	No exceptions noted.

CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Observed a Quarterly Access Review to determine there are access reviews conducted, access is modified based on business need, and sampled 2 of 2 access reviews to determine they are conducted quarterly. Inspected the Access Control and Termination Policy to determine access is restricted based on the principle of least privilege and changes are required to be approved and documented.	No exceptions noted.
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Observed a Screenshot of an Employee's Access Removal Procedures to determine there is a termination checklist followed and access is appropriately removed upon termination	No exceptions noted.
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Observed a New Account Checklist to determine access is granted based on job role Inspected the Access Control and Termination Policy to determine the principle of least privilege is followed and access is modified based on job need and must be approved.	No exceptions noted.
CC 6.3	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	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Observed a Screenshot of 1Password to determine users have unique authentication IDs. Inspected the Access Control and Termination Policy to determine users are required to have unique authorized authentication.	No exceptions noted.

	privilege and segregation of duties, to meet the entity's objectives.			
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners.	Inspected the System Description to determine AWS is responsible for restricting data center access to authorized personnel.	No exceptions noted.
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company reviews access to the data centers at least annually.	Inspected the System Description to determine there are periodic access reviews and AWS is responsible for restricting data center access to authorized personnel.	No exceptions noted.
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company requires visitors to sign-in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.	Inspected the Physical Security Policy to determine there are visitor management procedures documented that include signing in, wearing a name badge, escorted if necessary, access approval, and signing out. Inspected the System Description to determine AWS is responsible for handling physical security controls.	No exceptions noted.
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Observed a Quarterly Access Review to determine there are access reviews conducted, access is modified based on business need, and sampled 2 of 2 access reviews to determine they are conducted quarterly. Inspected the Access Control and Termination Policy to determine access is restricted based on the principle of least privilege and changes are required to be approved and documented. Inspected the System Description to determine AWS is responsible for handling physical security controls.	No exceptions noted.

CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Observed a Screenshot of an Employee's Access Removal Procedures to determine there is a termination checklist followed and access is appropriately removed upon termination	No exceptions noted.
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Observed Secureframe to determine there is a data disposal log maintained. Inspected the Data Retention and Disposal Policy to determine there are data disposal procedures documented that include following the Nist Guidelines.	Disclosure: no data or devices were disposed of during the audit window.
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected the Data Retention and Disposal Policy to determine there are data retention and disposal processes and procedures documented to assist with the secure retention or disposal of data and customer data is deleted within 30 days of request. Observed Secureframe to determine there is a disposal log used to assist with the secure disposal of company and customer data.	Disclosure: no data or devices were disposed of during the audit window.
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Retention and Disposal Policy to determine there are data retention and disposal processes and procedures documented to assist with the secure retention or disposal of data and customer data is deleted within 30 days of request. Observed Secureframe to determine there is a disposal log used to assist with the secure disposal of company and customer data.	Disclosure: no data or devices were disposed of during the audit window.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized	Observed a Screenshot of 1Password to determine users have unique authentication IDs. Inspected the Access Control and Termination Policy to determine	No exceptions noted.

		Secure Socket Shell (SSH) keys.	users are required to have unique authorized authentication.	
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Observed the CodeSee Website to determine HTTP requests are redirected to HTTPS and there is a valid certificate in use that indicates SSL is used.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Observed a Screenshot of GuardDuty being used and Configured to determine GuardDuty is used for threat detection, continuous monitoring, and detection of security breaches.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Observed a Screenshot of Kolide to determine there are firewalls used, reviewed periodically, and issues are communicated to authorized personnel so that they can be resolved..	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses firewalls and configures them to prevent unauthorized access.	Observed a Screenshot of Kolide to determine there are firewalls used and configured to prevent unauthorized access.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Observed a Screenshot of CloudFlare to determine authorized personnel are required to have and use MFA when accessing the production systems.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Observed the CodeSee Website to determine there is a valid web certificate in place and the connection is secured with SSL.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Observed a Penetration Test Report to determine there are penetration tests conducted and identified vulnerabilities are tracked to remediation. Inspected the Vulnerability and Patch Management Policy to determine patches are installed as part of routine maintenance and to ensure that systems are hardened against vulnerabilities and threats.	No exceptions noted.

CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Observed a Screenshot of CloudFlare being used to determine Cloudflare is used for network and system hardening. Inspected the Configuration and Asset Management Policy to determine there are hardening standards documented, are based on industry standards, and are reviewed periodically.	No exceptions noted.
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company encrypts portable and removable media devices when used.	Observed a Screenshot of Kolide to determine FileVault is enabled on employee workstations.	No exceptions noted.
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Observed the CodeSee Website to determine HTTP requests are redirected to HTTPS and there is a valid certificate in use that indicates SSL is used.	No exceptions noted.
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Observed Secureframe to determine Kolide is used for device management.	No exceptions noted.
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company deploys Anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Observed Secureframe to determine Kolide is used for device management, an inventory of devices is maintained that indicates if devices have antivirus enabled, and all devices have sufficient antivirus enabled.	No exceptions noted.

CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine there are processes and procedures for the development, engineering, security, checking, testing, implementing, version control, change control, and test data documented. Observed a Screenshot of GitHub to determine the SDLC is followed.	No exceptions noted.
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Observed a Penetration Test Report to determine there are penetration tests conducted and identified vulnerabilities are tracked to remediation. Inspected the Vulnerability and Patch Management Policy to determine patches are installed as part of routine maintenance and to ensure that systems are hardened against vulnerabilities and threats.	No exceptions noted.
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the Change Management Policy to determine the steps taken for software and infrastructure changes: product roadmap, planning, evaluating, building, testing, documenting, code reviewing, approval, implementing, communication, and post change review. Observed a Screenshot of changes on GitHub to determine changes are approved and that the change management process is followed.	No exceptions noted.
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Observed a Screenshot of GitHub to determine GitHub is used to manage configurations and verify configurations are deployed consistently throughout the environment.	No exceptions noted.
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that	The company's formal policies outline the requirements for the following functions related to IT / Engineering:	Observed a Penetration Test to determine there are penetration tests conducted. Observed a Screenshot of GuardDuty being used to determine there are system monitoring configurations	No exceptions noted.

	result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	- vulnerability management; - system monitoring.	enabled. Inspected the Vulnerability and Patch Management Policy to determine there are vulnerability management processes and procedures documented. Inspected the Information Security Policy to determine there are monitoring processes and procedures documented.	
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Observed Secureframe to determine there are risk assessments conducted, risks are identified and remediated, and a risk registry is maintained. Inspected the System Description to determine fraud is considered during the risk assessment process. Inspected the Risk Assessment and Treatment Policy to determine risk assessments are conducted annually or whenever there are significant changes.	No exceptions noted.
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. critical and high vulnerabilities are tracked to remediation.	Observed Secureframe to determine that there are vulnerability scans conducted, that findings are given severity ratings, and that they are tracked to remediation.	No exceptions noted.
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Observed a Screenshot of GuardDuty being used and Configured to determine GuardDuty is used for threat detection, continuous monitoring, and detection of security breaches.	No exceptions noted.
CC 7.2	The entity monitors system components and	The company utilizes a log management tool to identify	Observed a screenshot of log evidence to determine that event	No exceptions noted.

	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.	events that may have a potential impact on the company's ability to achieve its security objectives.	logs are maintained to assist with the achievement of security objectives.	
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Observed a Penetration Test Report to determine there are penetration tests conducted and identified vulnerabilities are tracked to remediation. Inspected the Vulnerability and Patch Management Policy to determine there are third-party penetration tests conducted at least annually.	No exceptions noted.
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Observed a Penetration Test to determine there are penetration tests conducted. Observed a Screenshot of GuardDuty being used to determine there are system monitoring configurations enabled. Inspected the Vulnerability and Patch Management Policy to determine there are vulnerability management processes and procedures documented. Inspected the Information Security Policy to determine there are monitoring processes and procedures documented.	No exceptions noted.
CC 7.2	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	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Observed a Penetration Test Report to determine there are penetration tests conducted and identified vulnerabilities are tracked to remediation. Inspected the Vulnerability and Patch Management Policy to determine patches are installed as part of routine maintenance and to ensure that systems are hardened against vulnerabilities and threats.	No exceptions noted.

	determine whether they represent security events.			
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Observed an Infrastructure Diagram to determine there are load balancers used. Inspected the Network Security Policy to determine there are IDS/IPS procedures documented that include configuring alerts when issues are met.	No exceptions noted.
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. critical and high vulnerabilities are tracked to remediation.	Observed Secureframe to determine that there are vulnerability scans conducted, that findings are given severity ratings, and that they are tracked to remediation.	No exceptions noted.
CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Policy to determine there are privacy and incident response processes and procedures documented and communicated to all necessary personnel.	No exceptions noted.
CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Observed Secureframe to find 11 of 11 eligible employees that have acknowledged the security incident response plan. Observed a Tabletop Exercise to determine incidents and issues are logged, tracked to remediation, and communicated to affected parties. A 12th employee started at CodeSee in February 2022 and is still within the SLA of	No exceptions noted.

			completing onboarding procedures as of this audit.	
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company tests their incident response plan at least annually.	Observed a Business Continuity and Disaster Recovery Tabletop Exercise to determine the incident response plan is tested. Inspected the Security Incident Response Plan to determine the incident response plan is tested as part of the disaster recovery tabletop Exercise and is tested annually.	No exceptions noted.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Policy to determine there are privacy and incident response processes and procedures documented and communicated to all necessary personnel.	No exceptions noted.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Observed Secureframe to find 11 of 11 eligible employees that have acknowledged the security incident response plan. Observed a Tabletop Exercise to determine incidents and issues are logged, tracked to remediation, and communicated to affected parties. A 12th employee started at CodeSee in February 2022 and is still within the SLA of completing onboarding procedures as of this audit.	No exceptions noted.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Observed a Penetration Test Report to determine there are penetration tests conducted and identified vulnerabilities are tracked to remediation. Inspected the Vulnerability and Patch Management Policy to determine patches are installed as part of routine maintenance and to ensure that systems are hardened against vulnerabilities and threats.	No exceptions noted.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. critical and high vulnerabilities are tracked to remediation.	Observed Secureframe to determine that there are vulnerability scans conducted, that findings are given severity ratings, and that they are tracked to remediation.	No exceptions noted.

	communicate security incidents, as appropriate.			
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business Continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Observed a Business Continuity and Disaster Recovery Tabletop Exercise to determine the business continuity and disaster recovery plan is tested. Inspected the Business Continuity and Disaster Recovery Plan to determine the plan is tested at least annually.	No exceptions noted.
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company tests their incident response plan at least annually.	Observed a Business Continuity and Disaster Recovery Tabletop Exercise to determine the incident response plan is tested. Inspected the Security Incident Response Plan to determine the incident response plan is tested as part of the disaster recovery tabletop Exercise and is tested annually.	No exceptions noted.
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Policy to determine there are privacy and incident response processes and procedures documented and communicated to all necessary personnel.	No exceptions noted.
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Observed Secureframe to find 11 of 11 eligible employees that have acknowledged the security incident response plan. Observed a Tabletop Exercise to determine incidents and issues are logged, tracked to remediation, and communicated to affected parties. A 12th employee started at CodeSee in February 2022 and is still within the SLA of completing onboarding procedures as of this audit.	No exceptions noted.
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the Change Management Policy to determine the steps taken for software and infrastructure changes: product roadmap, planning, evaluating, building, testing, documenting, code reviewing, approval, implementing, communication, and post change review. Observed a Screenshot of changes on GitHub to determine changes are approved and that the change management process is followed.	No exceptions noted.

CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company restricts access to migrate changes to production to authorized personnel.	Observed a Quarterly Access Review to determine access is reviewed and adjusted based on business need. Inspected the Access Control and Termination Policy to determine the principle of least privilege is followed and access is restricted based on business need.	No exceptions noted.
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine there are processes and procedures for the development, engineering, security, checking, testing, implementing, version control, change control, and test data documented. Observed a Screenshot of GitHub to determine the SDLC is followed.	No exceptions noted.
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Observed a Penetration Test Report to determine there are penetration tests conducted and identified vulnerabilities are tracked to remediation. Inspected the Vulnerability and Patch Management Policy to determine there are third-party penetration tests conducted at least annually.	No exceptions noted.
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Observed a Penetration Test Report to determine there are penetration tests conducted and identified vulnerabilities are tracked to remediation. Inspected the Vulnerability and Patch Management Policy to determine patches are installed as part of routine maintenance and to ensure that systems are hardened against vulnerabilities and threats.	No exceptions noted.
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Observed a Screenshot of CloudFlare being used to determine Cloudflare is used for network and system hardening. Inspected the Configuration and Asset Management Policy to determine there are hardening standards documented, are based on industry standards, and are reviewed periodically.	No exceptions noted.

CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. critical and high vulnerabilities are tracked to remediation.	Observed Secureframe to determine that there are vulnerability scans conducted, that findings are given severity ratings, and that they are tracked to remediation.	No exceptions noted.
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security Continuity in the event of the unavailability of key personnel.	Observed the Business Continuity and Disaster Recovery Tabletop Exercise to determine there are communication plans tested in the event of the unavailability of key personnel. Inspected the Business Continuity and Disaster Recovery Plan to determine there are alternate communication processes and procedures documented.	No exceptions noted.
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected the Risk Assessment and Treatment Policy to determine insurance is considered during the risk treatment process as part of transferring risk.	No exceptions noted.
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Observed Secureframe to determine there are risk assessments conducted, risks are identified and remediated, and a risk registry is maintained. Inspected the System Description to determine fraud is considered during the risk assessment process. Inspected the Risk Assessment and Treatment Policy to determine risk assessments are conducted annually or whenever there are significant changes.	No exceptions noted.
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Assessment and Treatment Policy to determine the risk management processes and procedures of scoping assets, identification of threats and vulnerabilities, analysis of risk, risk treatment, calculation of residual risk, and reporting are documented. Observed Secureframe to determine there is a risk registry maintained with	No exceptions noted.

			identified vulnerabilities, vulnerabilities are given severity ratings, and vulnerabilities are tracked to remediation.	
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Observed a sample Signed Non Disclosure Agreement to determine there are confidentiality and privacy agreements made with contractors and third-parties.	No exceptions noted.
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Observed Secureframe to determine there is a vendor list maintained where vendors are given severity ratings, hve security and privacy requirements, and have reviews conducted periodically. Inspected the Vendor Management Policy to determine there are contract reviews that review contractor privacy and security commitments., annual vendor reviews, risk assessment, and due diligence procedures documented.	No exceptions noted.