KEYTOS

SOC 2 Type 2 Report

Keytos LLC

April 16, 2022 to April 16, 2023
Next Report Issue Date: June 15, 2024

A Type 2 Independent Service Auditor’s Report on Controls Relevant to Security

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

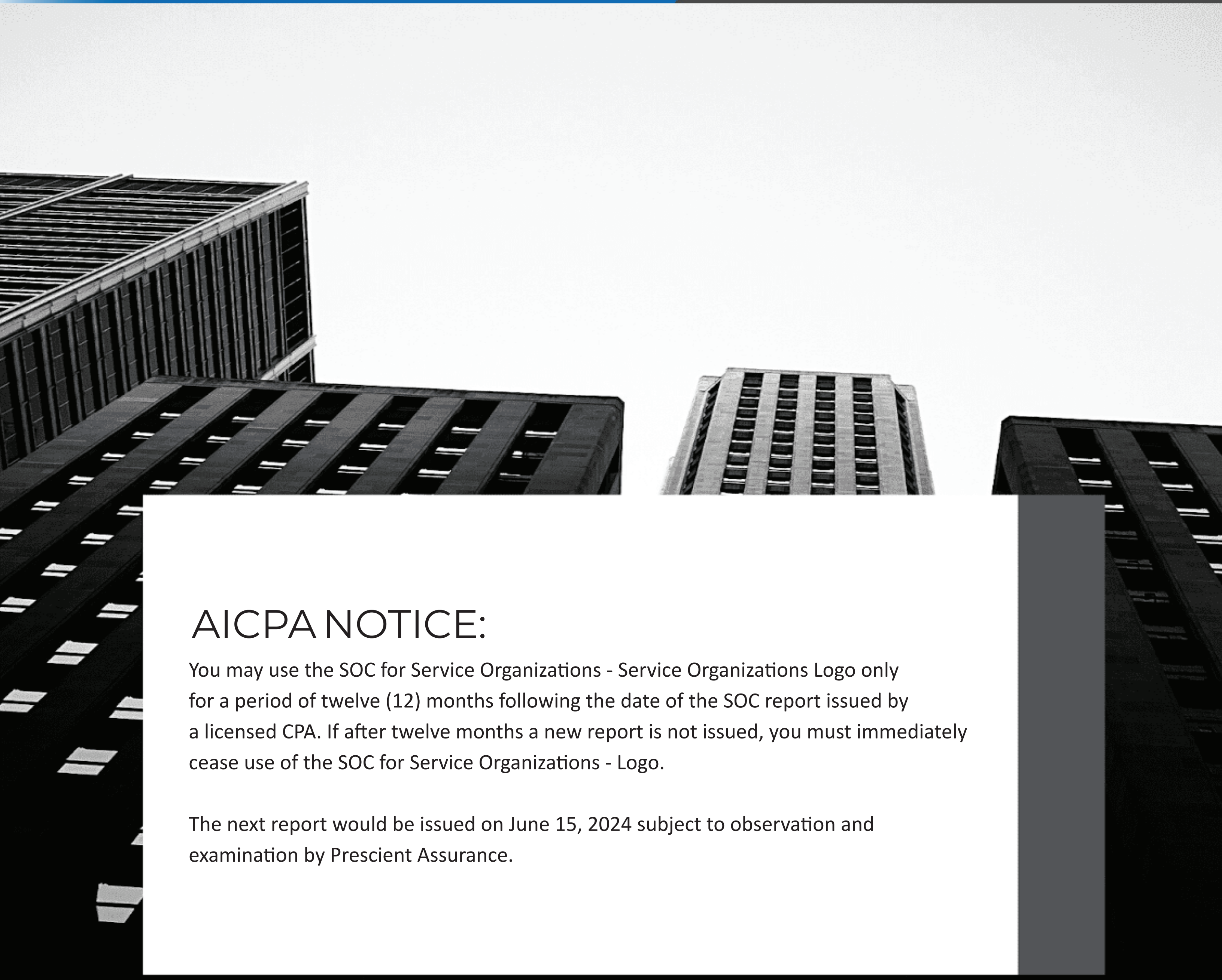
AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

CPA

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

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



AICPA NOTICE:

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

The next report would be issued on June 15, 2024 subject to observation and examination by Prescient Assurance.

Table of Contents

SECTION 1

Management's Assertion

Management's Assertion

We have prepared the accompanying description of Keytos LLC's system throughout the period April 16, 2022, to April 16, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. The description is intended to provide report users with information about Keytos LLC's system that may be useful when assessing the risks arising from interactions with Keytos LLC's system, particularly information about system controls that Keytos LLC 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*.

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

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

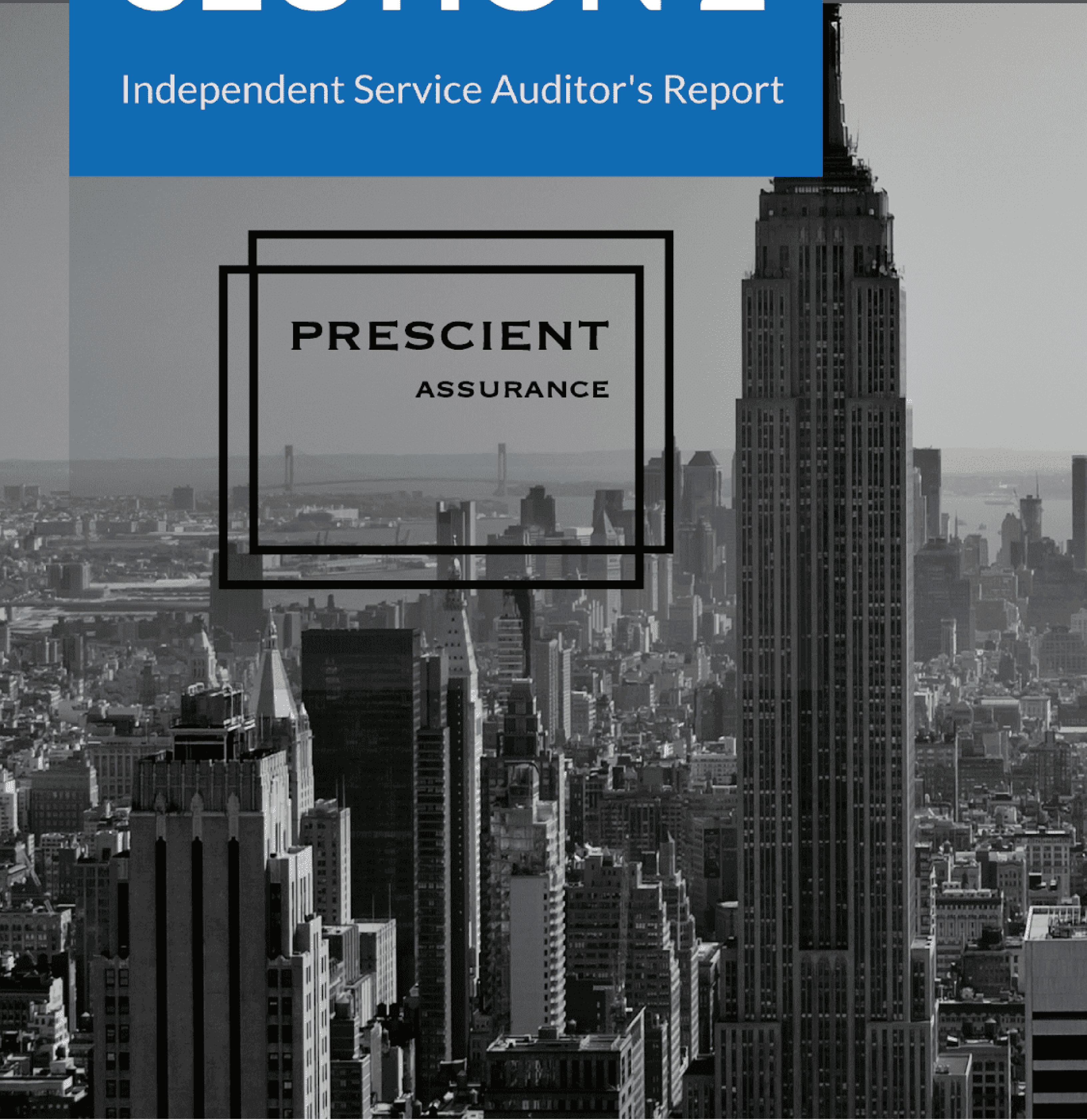
a. The description presents Keytos LLC's system that was designed and implemented throughout the period April 16, 2022, to April 16, 2023 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period April 16, 2022, to April 16, 2023, to provide reasonable assurance that Keytos LLC'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 Keytos LLC's controls during that period.
c. The controls stated in the description operated effectively throughout the period April 16, 2022, to April 16, 2023, to provide reasonable assurance that Keytos LLC's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of Keytos LLC's controls operated effectively throughout the period.

DocuSigned by:
Igal Flegmann
B1A73A220656499...

Igal Flegmann
CEO
Keytos LLC

SECTION 2

Independent Service Auditor's Report



PRESCIENT

ASSURANCE

Independent Service Auditor's Report

To: Keytos LLC

Scope

We have examined Keytos LLC's ("Keytos LLC") accompanying description of its EZSSH system found in Section 3, titled Keytos LLC System Description throughout the period April 16, 2022, to April 16, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 16, 2022, to April 16, 2023, to provide reasonable assurance that Keytos LLC'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*.

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

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

Service Auditor's Responsibilities

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

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

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

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

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

Inherent Limitations

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

Opinion

In our opinion, in all material respects:

a. The description presents Keytos LLC's system that was designed and implemented throughout the period April 16, 2022, to April 16, 2023, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period April 16, 2022, to April 16, 2023, to provide reasonable assurance that Keytos LLC'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 Keytos LLC's controls throughout the period.
c. The controls stated in the description operated effectively throughout the period April 16, 2022, to April 16, 2023, to provide reasonable assurance that Keytos LLC's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Keytos LLC's controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of Keytos LLC, user entities of Keytos LLC's system during some or all of the period April 16, 2022 to April 16, 2023, business partners of Keytos LLC subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Prescient Assurance LLC

DocuSigned by:
John D Wallace
F5ADFA3569EA450... --

John D. Wallace, CPA
Chattanooga, TN
June 15, 2023

SECTION 3

System Description

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

"Keytos LLC" is a cyber security company that offers Identity Management and PKI services to customers using its SAAS platform or expert resources. We decrease the identity management costs while improving company security by issuing short-term certificates to access resources; removing the need of managing and rotating credentials. Keytos LLC was founded in 2021. We have 15+ customers across the globe and consist of NYSE-listed companies to small startups. Our environments are protected by security controls that have undergone numerous audits for SOC-2.

Keytos LLC provides a SAAS UI/APIs/Plug-ins/Managed Services which include:

- ***Identity Management Services:*** *Providing companies an easy-to-use Identity management service that allows companies to extend their corporate identity protections to SSH endpoints and GitHub accounts by using the corporate identity to issue short term SSH certificates that provide just in time access to the customer's infrastructure and GitHub repositories.*
- ***PKI As a Service:*** *Providing companies an easy way to create and manage SSL certificates for their passwordless strategy.*

DC 2: The Principal Service Commitments and System Requirements

Keytos LLC designs its processes and procedures to meet the objectives of reducing IT cost while improving security by making easy to use security tools. Those objectives are based on the service commitments that Keytos LLC makes to user entities, the laws and regulations that govern the provision of services, and the financial, operational, and compliance requirements that Keytos LLC has established for the services. The services of Keytos LLC are subject to the federal and state privacy and security laws and regulations in the jurisdictions in which Keytos LLC operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. https://www.keytos.io/. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Keytos 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.
- Regularly scanning the cloud infrastructure and reporting any anomalies.

Keytos LLC 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 Keytos LLC's Terms and Conditions https://www.keytos.io/Legal/TermsOfUse.txt 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 is 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 EZSSH Platform.

2.1 Support SLA

Severity	Response Time
Severity 1, Critical: ● Access to Keytos LLC Portal in production is down.	<1 Hour For Business Criticalcustomers. <24 hours for Premium Support customers. One business day for Basic Support customers.
Severity 2, High: ● Production issue where the system is functioning but in degraded or restricted capacity. ● At least 25% of containers and hosts in the application are in an unhealthy state.	<1 Hour For Business Criticalcustomers. <24 hours for Premium Support customers. One business day for Basic Support customers.
Severity 3, Medium: ● Production issue where minor functionality is impacted or a development issue.	<1 Hour For Business Criticalcustomers. <24 hours for Premium Support customers. One business day for Basic Support customers.
Severity 4, Low: ● Request for information with no impact to business operations	Next Business Day*

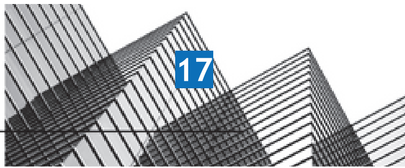
DC 3: The Components of the System Used to Provide the Services

3.1 Primary Infrastructure

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Azure	Azure Web Applications IAM Load Balancers	Allow for the servicing, processing, and directing of network traffic and data. Allow management of user accounts.
Azure	Azure Security Center	Used for monitoring network resources and alerting based on preconfigured metric-based alarms.
Azure	Azure SQL Cosmos DB	Used to store user and customer data.
GitHub	Codebase & CICD/Pipeline	Codebase used for versioning, testing, and deployment of changes to the environments.
Github Issues	Communication Services	Internal business communications, storage of organizational documents, and project management.
Azure	Azure Key Vault	Protects the customer cryptographic keys with Hardware Security Modules.
Azure	Application Insights	Application logs for all of the services

3.2 Primary Software

Primary Software		
Software	**Type**	**Purpose**
C#	Server Side Logic	Primary development language/runtime for all applications



Primary Software		
Software	**Type**	**Purpose**
Blazor/C#	UI Logic	Web application framework used to power the web application/sync configuration tool
Azure Functions	Functions	Handle async tasks such as sending email, updating meetered use, etc.
Azure SQL	Database	Transactional database for customer data

3.3 People

Keytos LLC has a staff of approximately 3 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 Keytos 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 Keytos 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.
- **Infrastructure:** DevOps provides technical assistance to Keytos LLC's developers and maintains the cloud infrastructure that the Keytos product runs on.
- **Security**: Employees or outsourced Individuals responsible for providing ongoing security to Keytos LLC's assets (people, application, infrastructure, and data).
- **IT and Customer Support**: Individuals responsible for providing timely resolution of issues and problems.
- **Sales and customer success:** reach out to potential customers and help them adopt Keytos products.

3.4 Security 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:

Keytos application runs in the Azure Cloud utilizing Azure Web apps, Storage, and Database services.

- Each platform instance (production, test, development) is contained within a separate Azure tenant. 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 MFA controlled access.

Access is granted on a project and component within each project (i.e., pods, storage, and database) basis.

- Data is persisted in both Azure Storage and SQL Services. Both utilize Advanced Encryption Standard ("AES") 256 encrypted disks for all data stored at rest. Each customer instance in production establishes a logical database that is allocated for use solely for that customer. Customer data is never co-mingled in the EZSSH application.
- User entities access their instance 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 in-person 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.

3.5 Data

There are five major types of data used by Keytos LLC.

Principal Data Types	
Data Types	**Protection and Breach Notification during the lifecycle of Data**
Configuration Data: Data used to configure Keytos System	Configuration Data is stored in SQL databases and includes the names of databases, schemata, tables, columns, custom objects, and custom fields; and models (SQL queries) stored by customers to provide custom analysis views, and routines in the web-based software application.
Log Data: Logs produced by the Keytos	Log Data is produced by the various services to make it easier for Keytos LLC operators to monitor the health of the system and track down any issues. Log data may be stored by vendors (Microsoft) that Keytos LLC has entrusted for purposes like indexing, monitoring, and trending. Log data is retained for one year.

Principal Data Types	
Data Types	**Protection and Breach Notification during the lifecycle of Data**
Service Data	Service Data is user and account metadata, troubleshooting, accounts receivable and billing, and related information necessary for the Company to know to service accounts and provide the Service.
Data in transit	To protect data in transit between our app and our servers, Keytos LLC 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 Keytos LLC's production network is encrypted using industry-standard 256-bit Advanced Encryption Standard (AES256), which applies to all types of data at rest within Keytos LLC's systems—relational databases, file stores, database backups, etc.

3.6 Third Party

Services	Service usage
Microsoft	Azure Cloud, Office 365 for email and file sharing, Microsoft Clarity for user analytics.
GitHub	Code management and CI/CD Deployment

3.7 System Boundaries

The boundaries for the Keytos system audit are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of this audit.

DC 4: Disclosures about Identified Security Incidents

No significant incidents have occurred to the services provided to user entities during the review period or since the organization's last review.

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

5.1 Integrity and Ethical Values

Keytos LLC 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. Keytos LLC has also instituted a number of technical controls to prevent and disincentivize illegal and unethical actions by Keytos LLC employees. These controls include but are not limited to:

- Logging all traffic within Keytos LLC'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 Keytos LLC management.
- Use of NDAs to prevent the disclosure of confidential information to unauthorized parties.

5.2 Commitment to Competence

Keytos LLC'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.

5.3 Management's Philosophy and Operating Style

Keytos LLC'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 Keytos LLC has instituted a number of processes:

- Weekly "all hands" meetings for employees to voice their blocks, successes, and concerns.
- A rigorous QA program ensuring that development on the Keytos LLC 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.

5.4 Organizational Structure and Assignment of Authority and Responsibility

During normal operations Keytos LLC has a simple organizational structure. Employees report directly to the CEO who ultimately provides direction. Keytos LLC 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. Keytos LLC 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.

5.5 Human Resource Policies and Practices

Keytos LLC consistently strives to hire and retain the most qualified individuals for the job. To meet this goal, Keytos LLC 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, Keytos LLC 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" which is given to new hires and is fully accessible to all Keytos LLC employees
- Lastly, Keytos LLC 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.
- Weekly Employee training where a leader of our team presents on one of the latest security topics that are related to the company and industry.

5.6 Security Management

The 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. They are responsible for enforcing the information security policies, configuring, monitoring, and maintaining preventative, corrective, and detective controls within the Keytos LLC environment, and ensuring user awareness training is conducted.

As the information security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses 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 IT maintenance 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.

5.7 Security Policies

Keytos LLC has adopted the following Security Policies:

- Access Control Policy
- Asset Management Policy
- Business Continuity and Disaster Recovery Plan
- BYOD Policy
- Code of Conduct
- Cryptography Policy
- Data Management Policy
- Human Resource Security Policy
- Incident Response Plan
- Information Security Policy (AUP)
- Information Security Roles and Responsibilities
- Operations Security Policy
- Risk Management Policy
- Secure Development Policy

5.8 Personnel Security

Keytos LLC 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 Keytos LLC employees.
- Employees are directed to report any potential security incidents to the IT Manager.
- Violations of Keytos LLC security policies have clearly defined repercussions.

5.9 Physical Security and Environmental Controls

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

5.10 Change Management

Keytos LLC's change management procedures are detailed in the Operations Security Policy. There are five requirements for all changes to the organization, business processes, information processing facilities, and systems that affect information security in Keytos LLC's production environment. They are as follows:

- The change must include processes for planning and testing of changes, including remediation measures.
- Documented managerial approval and authorization before proceeding with changes that may have a significant impact on information security, operations, or the production platform.
- Advance communication/warning of changes, including schedules and a description of reasonably anticipated effects, provided to all relevant internal and external stakeholders.
- Documentation of all emergency changes and subsequent review.
- A rollback process for unsuccessful deployments must be in place.

5.11 System Monitoring

Keytos LLC uses a combination of services to monitor its network and systems. These include CloudWatcher, the Drata Client, Azure Security Center, and Azure AppInsights.

- CloudWatcher: Is used to monitor the Azure infrastructure and detect any changes compared to the baseline approved by the security team.
- Compliance Automation Platform Client: Compliance Automation Platform allows us to monitor multiple aspects of our attack surface including employee devices (ensuring anti-malware, HDD encryption, etc. are in place), monitoring Azure resources for potential configuration vulnerabilities, and tracking necessary patches/updates.
- Azure Security Center (Defender for Cloud) Used for monitoring of network usage, availability, and overall performance and health of network resources. Also logs metrics for fine-tuning alarms and alerts as usage data is received. Amazon CloudWatch Logs are used in conjunction with AWS CloudTrail to monitor failed and successful authorization attempts.
- Azure Application Insights: Used to log actions taken by users and services within our AWS account.

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

5.12 Incident Management

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

Specific steps that Keytos LLC will take are:

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

5.13 Data Backup and Recovery

Keytos LLC uses redundant Azure SQL instances to ensure full backup recovery of its database. For local files of employee workstations, Keytos LLC employees use OneDrive which acts as a backup. Access to Keytos LLC databases is heavily restricted using role-based authorization controls.

5.14 System Account Management

Keytos LLC's access management procedures are documented in its Access Control Policy. Keytos LLC uses Role-based authorization to control access to its network infrastructure. Keytos LLC uses the principle of least privilege to determine the type and level of access to grant users. A number of standards are in place which Keytos LLC uses when granting access to its systems:

- Technical access to Keytos LLC networks must be formally documented.
- Background checks will be performed on domestic people granted access to Keytos LLC networks.
- Only authorized Keytos LLC employees and third parties working off a signed contract or statement of work, with a business need, shall be granted access to the Keytos LLC production network.

With regards to access provisioning, Keytos LLC uses the following controls:

- New employees and/or contractors are not to be granted access to any Keytos LLC production systems until after they have completed all HR onboarding tasks, which includes receiving and passing a background check (as applicable), review and signing of all company policies, signing of Keytos LLC's NDA, and completion of cybersecurity awareness training.
- Access is restricted to only what is necessary to perform job duties.
- No access may be granted earlier than the official employee start date.
- Access requests and rights modifications shall be documented in an access request ticket or email. No permissions shall be granted without approval from the system/data owner or management.
- Records of all permission and privilege changes shall be maintained for no less than one year.
- Access rights of users must be removed promptly within 24 hours of notification being given to the IT Manager.

- If current access rights are no longer needed due to transfer or change of role, termination of those rights must be performed promptly within 24 hours of notification being given to the IT Manager.

5.15 Risk Management Program

5.15.1 Data Classification

Keytos LLC has three classifications for the data it uses, processes, and produces. The classifications are **Confidential, Restricted, and Public.**

Confidential Data is considered highly sensitive and has heavy restrictions spelled out in Keytos LLC's Data Management Policy. Examples include:

- PII
- PHI
- Customer Data
- Keytos LLC financial and banking data
- Incident Reports
- Risk Assessment Reports
- Technical Vulnerability Reports
- Secret and Private Keys
- Source Code

Restricted Data is defined as proprietary information requiring thorough protection. Access to this data is restricted to employees on a "need-to-know" basis. Approval is required for distribution. Examples include:

- Internal Policies
- Legal Documents
- Internal Reports
- Slack Messages
- Emails
- Contracts
- Bug Reports and Maintenance

Public Data is defined as: Documents intended for public consumption which can be freely distributed outside of Keytos LLC. Examples include:

- Marketing Materials
- Product Descriptions
- Release Notes
- External Facing Policies

5.15.2 Risk Management Responsibilities

Keytos LLC's Risk Management Policy details the primary responsibilities.

Risk Management	
Role	**Responsibility**
CEO	Ultimately responsible party for the acceptance and/or treatment of any risks to the organization.

Risk Management Policy

Keytos LLC's Risk Management Policy is designed to be used as an integral part of the strategic and operational goals of the organization. To accomplish this Keytos LLC has developed a process to identify the risks which would hinder the achievement of its objectives. The majority of responsibility falls to the IT Manager including the enforcement of policy requirements, application of policy requirements to Keytos LLC systems, and the reporting of any non-compliance to the appropriate entities.

In general, risks are assessed along two metrics: impact and likelihood of occurrence. This process may be applied to all business processes, information systems, employees, vendors, and any other affiliates.

To this end, Keytos LLC completes multiple assessments and tests on an annual basis including black hat penetration tests, white hat penetration tests, and a risk assessment. These tests are meant to inform Keytos LLC's understanding of its attack surface as well as illuminate potentially unrealized vulnerabilities. With this in mind, a third party will perform the penetration tests. The risk assessment will be performed by Keytos LLC's internal team.

The results of the risk assessment are tracked and logged in Keytos LLC's Drata client and remediation plans/efforts will also be tracked in the Drata client.

5.15.3 Risk Management Program Activities

On a practical level, Keytos LLC's Risk Management process involves **3 stages**: identification of risks, assessment of their potential impact, and Keytos LLC'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**.

The risk assessment focuses on the likelihood and potential impact of risks to Keytos LLC. Likelihood can be assessed as not likely, somewhat likely, or very likely. The impact can be assessed as not impactful, somewhat impactful, and very impactful. These factors together will give an overall risk ranking.

Keytos LLC's stance towards any given risk is based on the assessment described above. Where Keytos LLC chooses a risk response other than "Accept," it shall develop a Risk Treatment Plan. Keytos LLC's stance will fall into one of the following categories:

- **Mitigate:** Keytos LLC may take actions or employ strategies to reduce the risk.
- **Accept**: Keytos LLC 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**: Keytos LLC 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 Keytos LLC, or insurance may be appropriate for protection against financial loss.
- **Eliminate**: The risk may be such that Keytos LLC could decide to cease the activity or to change it in such a way as to end the risk.

Keytos LLC's Business Continuity and Disaster Recovery Plan details our key business processes and critical services.

Risk Assessment

Keytos LLC'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, PII, or PHI.
- Potential monetary loss.
- The ability of the risk to impact Keytos LLC's business objectives.
- Potential impact to Keytos LLC customers or vendors.

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

Risk Analysis

Keytos LLCs Risk Analysis Method is as follows:

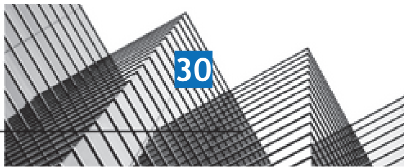
	RISK = LIKELIHOOD * IMPACT	LIKELIHOOD		
		Very likely: 3	Somewhat likely: 2	Not likely: 1
IMPACT	Very impactful: 3	9	6	3
	Somewhat impactful: 2	6	4	2
	Not impactful: 1	3	2	1

RISK LEVEL	RISK DESCRIPTION
Low (1-2)	A threat event could be expected to have a limited adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations.

RISK LEVEL	RISK DESCRIPTION
Moderate (3)	A threat event could be expected to have a serious adverse effect on organizational operations, mission capabilities, assets, individuals, customers or other organizations
High (7-9)	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
Not impactful (1)	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.
Somewhat impactful (2)	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.
Very impactful (3)	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
Not likely (1)	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.
Somewhat likely (2)	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.
Very likely (3)	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 Keytos LLC's Risk Management Policy, risks will be prioritized and mapped according to the descriptions listed above. The following responses to risk should be employed. Where Keytos LLC chooses a risk response other than "Accept," it shall develop a Risk Treatment Plan.

- **Mitigate:** Keytos LLC may take actions or employ strategies to reduce the risk.
- **Accept:** Keytos LLC 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:** Keytos LLC 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 Keytos LLC, or insurance may be appropriate for protection against financial loss.
- **Eliminate:** The risk may be such that Keytos LLC could decide to cease the activity or to change it in such a way as to end the risk.

5.15.4 Integration with Risk Assessment

Keytos LLC 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 Keytos LLC to develop specialized controls. Keytos LLC takes into account all relevant factors; contractual, legal, and regulatory when designing these controls. Keytos LLC's VP of IT has the final say on the design and implementation of these controls.

In general, Keytos LLC's Risk Assessment procedure is still applicable to risks inherent in Keytos LLC's commitments and contractual responsibilities and should be applied to determining the severity of risks.

5.16 Information and Communications Systems

Keytos LLC uses Microsoft Teams for restricted internal communications. Keytos LLC also uses video conferencing tools and a company Office365 for both internal and external communications.

For workflow, project management, and sharing of internal documents Keytos LLC uses Github as well as a company share point Drive.

5.17 Data Communication

Keytos LLC uses a zero trust model where all network assets are protected by a strong identity perimeter as well as a network boundary on applicable resources. Specific IP addresses must be added to the firewall when interacting with production assets and no standing access is allowed.

Access Control to the production code base is limited via the following controls:

- Short term SSH Certificates must be issued to modify the codebase.
- The production code branch is protected, only with approval of a C-level executive can changes be added or deployed.
- RBAC approach is used for accessing the application code repository.
- All default regular-user accounts have been removed.

5.18 Monitoring Controls

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

5.18.1 Internal Monitoring

Keytos LLC has a highly interconnected business process allowing for visibility and insight by management into the operations of each department. Keytos leverages Microsoft monitoring tools to monitor the security of the organization as well as our own internal tools to augment this visibility.

5.18.2 Third Party Monitoring

Keytos LLC uses the Drata client to monitor for new vulnerabilities. The Drata client is also used for tracking and logging known vulnerabilities.

Our Code and CI/CD pipelines are monitored by GitHub's advanced security features as well as StepSecurity's CI/CD pipeline monitoring agent that ensures only known endpoints are being called during our build process.

The process for reporting of any deficiencies with regards to Keytos LLC policies and procedures is clearly spelled out in each relevant policy.

DC 6: Complementary User Entity Controls (CUECs)

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

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 Keytos LLC.
- User entities are responsible for maintaining the security of the identities used to access Keytos tools.
- User entities are responsible for notifying Keytos LLC 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 Keytos LLC 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 Keytos LLC services.
- User entities are responsible for immediately notifying Keytos LLC 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 Keytos LLC 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 Keytos LLC’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 Keytos LLC.
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 Keytos LLC.

DC 7: Complementary Subservice Organization Controls (CSOCs)

Keytos LLC uses Azure as a subservice organization for cloud services. Keytos LLC'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 Azure.

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 Azure related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. Azure physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities. Management of Keytos LLC receives and reviews the Azure SOC 2 report annually. In addition, through its operational activities, Keytos LLC management monitors the services performed by Azure 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 Azure management.

It is not feasible for the criteria related to the System to be achieved solely by Keytos LLC. Therefore, each user entity's internal control must be evaluated in conjunction with Keytos LLC'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	Azure is responsible for restricting data center access to authorized personnel.
CC6.4	Azure is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC7.2	Azure is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2	Azure is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2	Azure is responsible for overseeing the regular maintenance of environmental protections at data centers.

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

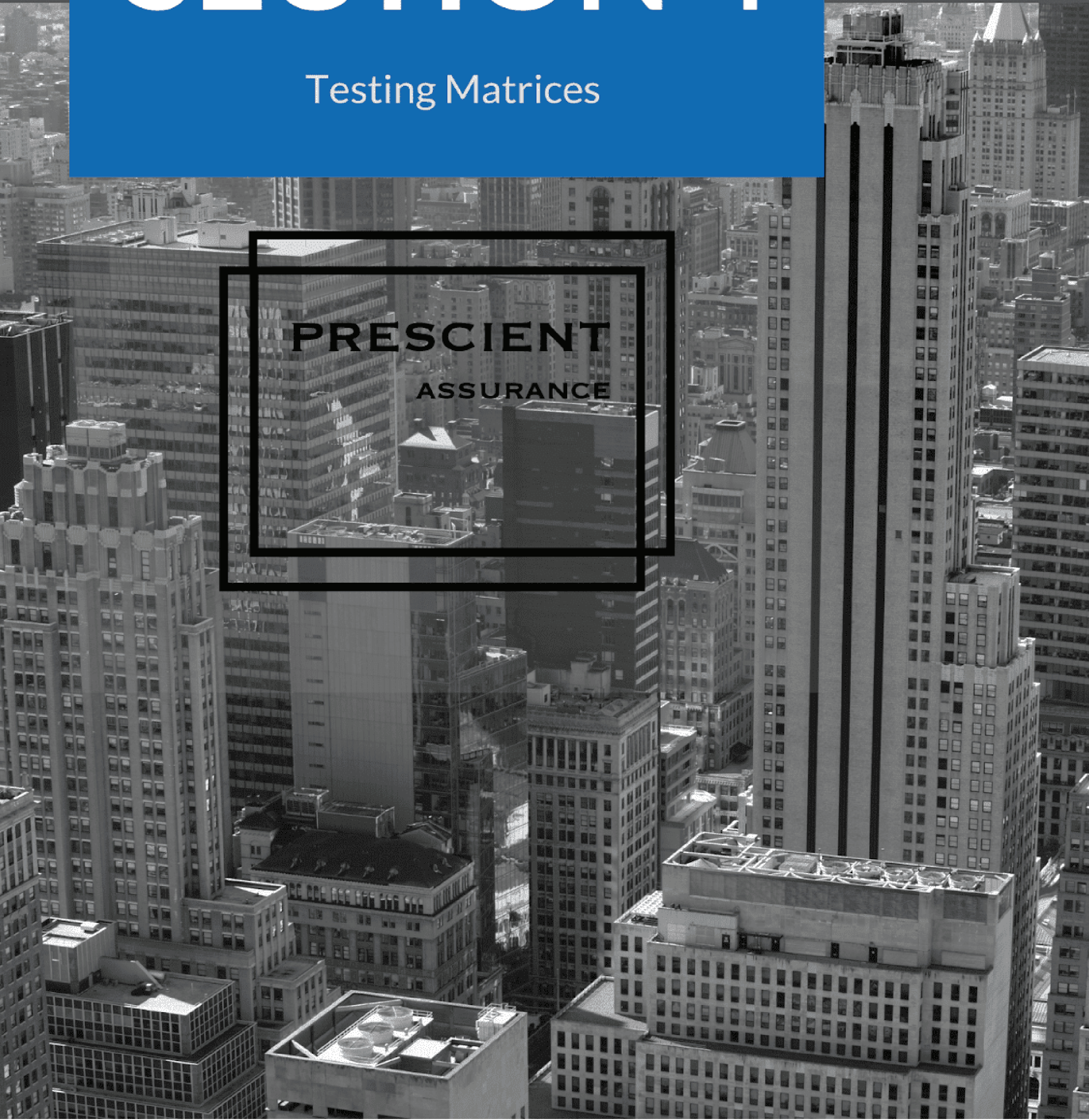
All Security criteria were applicable to the Keytos LLC system.

DC 9: Disclosures of Significant Changes In Last 1 Year

No significant changes have occurred in the last 1 year.

SECTION 4

Testing Matrices



PRESCIENT ASSURANCE

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

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

Prescient Assurance LLC conducted the examination testing throughout the period April 16, 2022, to April 16, 2023.

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

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

Types of Tests Generally Performed

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

Test Types	Description of Tests
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Inspection	Inspected documents and records indicating 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 the American Institute of Certified Public Accountants (AICPA) authoritative literature, Prescient Assurance utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, to determine the number of items to be selected in a sample for a particular test. Prescient Assurance, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

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

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

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

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

Reliability of Information Provided by the Service Organization

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

Test Results

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

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

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

Trust ID	COSO Principle	Control Description	Test Applied by the Service Auditor	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Keytos has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire.	Inspected the Acceptable Use Policy, which specifies the acceptable use of end-user computing devices and technology, to determine that the company has policies and procedures in place to establish acceptable use of information assets. Additionally reviewed the policy acknowledgment data to determine that all employees have accepted the company's Acceptable Use Policy.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Keytos's new hires are required to pass a background check as a condition of their employment.	Inspected the Acceptable Use Policy to determine that background verification checks on all candidates for employees and contractors should be carried out in accordance with relevant laws, regulations, and ethics. Disclosure: No full-time employee was on-boarded during the observation window.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Keytos requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.	Inspected the Code of Conduct to determine that all contractors are required to read and accept its terms. Inspected the Acceptable Use Policy to determine that all contractors are required to clear background checks and accept the terms of the policy. Disclosure: No contractors are included in the current workforce.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Keytos Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected the personnel data to determine that all policies have been approved by the management and that current employees and contractors have accepted the policies. Inspected the Information Security Policy to determine that all ISP policies are required to be reviewed,	No exceptions noted.

			modified, or edited by management annually and accessible to employees.	
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Keytos has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	Inspected the Code of Conduct to determine that the company has defined the ethical standards that all personnel are required to follow while performing their duties. Additionally reviewed the policy acknowledgment data to determine that all employees have accepted the company Policies.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Keytos has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.	Inspected the Data Protection Policy to determine that the company has established a Data Protection Policy. Observed records of policy to determine that most of the relevant employees have accepted the policy.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Keytos has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the list of key personnel to determine that the company has designated a security committee comprising one member.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	Inspected the Information Security Policy to determine that management has established defined roles and responsibilities to oversee the implementation of the information security policy across the organization.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Keytos engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected an application penetration test report issued by Prescient Security to determine that the company engages with a third-party to conduct penetration tests of the production environment at least annually. Inspected the Vulnerability	No exceptions noted.

			Management Policy to determine that penetration testing is required to be performed regularly by a penetration tester on Keytos's security team or an independent third party.	
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Keytos engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the quarterly code scans in GitHub to determine that quarterly vulnerability scans are performed at the company. Inspected the Vulnerability Management Policy to determine that the company requires all production systems to be scanned for vulnerabilities at least quarterly	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Management reviews security policies on an annual basis.	Inspected the policy list to determine that the Information Security Policy, Acceptable Use Policy, Physical Security Policy, Asset Management Policy, Incident Response Plan, System Access Control Policy, Encryption Policy, Data Protection Policy, and other security policies have been reviewed and approved on August 29, 2022. Inspected the Information Security Policy to determine that the company requires all ISPs to be reviewed, modified, and/or edited to meet necessary security standards.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.	Inspected the board members overview document which states brief information regarding board members, the information includes experience, accomplishments and skills to determine that the company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls.	No exceptions noted.
CC1.2	The board of directors demonstrates	Members of the Board of Directors are independent of management.	Inspected the profiles of the board members to determine that the board	No exceptions noted.

	independence from management and exercises oversight of the development and performance of internal control.		includes an advisor who is independent of management.	
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	Inspected the board meeting notes held on 10/25/22 to determine that the company's board of directors is briefed by senior management at least annually. The meeting minutes include discussions on preparing for additional compliance frameworks.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	Inspected the board meeting notes held on 10/25/22 to determine that the company's board of directors is briefed by senior management at least annually. The meeting minutes include discussions on preparing for additional compliance frameworks. Additionally, observed the Linkedin profiles of the board members to determine that the company board includes members who are independent of the company.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Keytos conducts a Risk Assessment at least annually.	Inspected a sample of annual risk assessments reports detailing risk assessment approach, risk score matrix, results, and treatment plan to determine that the company conducts annual risk assessments. Inspected the Risk Assessment Policy to determine that the company's risk assessment report is required to be updated when newly identified risks are identified and that the report should be updated and reviewed at least once per year.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate	Keytos reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Inspected the organization chart to determine that the company is headed by the CEO, and the Business Development and Head of Marketing report directly to the CEO.	No exceptions noted.

	authorities and responsibilities in the pursuit of objectives.			
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Keytos has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the list of key personnel to determine that the company has designated a security committee comprising one member.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Keytos's new hires are required to pass a background check as a condition of their employment.	Inspected the Acceptable Use Policy to determine that background verification checks on all candidates for employees and contractors should be carried out in accordance with relevant laws, regulations, and ethics. Disclosure: No full-time employee was on-boarded during the observation window.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Keytos's new hires and/or internal transfers are required to go through an official recruiting process during which their qualifications and experience are screened to ensure that they are competent and capable of fulfilling their responsibilities.	Observed a sample of a job applicant on Linkedin who was hired in December to determine that they went through an official recruiting process during which their qualifications and experience were screened to ensure that they are competent and capable of fulfilling their responsibilities.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Keytos evaluates the performance of all employees through a formal, annual performance evaluation.	Inspected a sample of employee annual review conversation reports to determine that the company evaluates the performance of all employees through a formal performance evaluation at least annually.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop,	All Keytos positions have a detailed job description that lists qualifications, such as requisite skills and experience,	Inspected the job descriptions for open positions on the company's website to determine that the company posts formal job	No exceptions noted.

	and retain competent individuals in alignment with objectives.	which candidates must meet in order to be hired by Keytos.	descriptions including the required skills and qualifications a candidate must meet in order to be hired, and evaluates the job candidates against the selection criteria. Inspected the job description for the position of an engineer to determine that the company maintains detailed job descriptions for job positions including the required skills and experiences that candidates must meet to get hired.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Keytos has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Keytos's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	Inspected the Information Security Policy to determine that the company requires all new hires to complete information security awareness training as part of the onboarding process and annually thereafter.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Keytos has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	Inspected the Code of Conduct to determine that the company has defined the ethical standards that all personnel are required to follow while performing their duties. Additionally reviewed the policy acknowledgment data to determine that all employees have accepted the company Policies including the Code of Conduct.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Keytos requires its contractors to read and accept the Code of Conduct, read and accept the Acceptable Use Policy, and pass a background check.	Inspected the Code of Conduct to determine that all contractors are required to read and accept its terms. Inspected the Acceptable Use Policy to determine that all contractors are required to clear background checks and accept the terms of the policy.	No exceptions noted.

			Disclosure: No contractors are included in the current workforce.	
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Keytos has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	Inspected the Code of Conduct to determine that the company has defined the ethical standards that all personnel are required to follow while performing their duties. Additionally reviewed the policy acknowledgment data to determine that all employees have accepted the company Policies including the Code of Conduct.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Keytos has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Keytos's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	Inspected the Information Security Policy to determine that the company requires all new hires to complete information security awareness training as part of the onboarding process and annually thereafter.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Keytos has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire.	Inspected the Acceptable Use Policy, which specifies the acceptable use of end-user computing devices and technology, to determine that the company has policies and procedures in place to establish acceptable use of information assets. Additionally reviewed the policy acknowledgment data to determine that all employees have accepted the company's Acceptable Use Policy.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Keytos evaluates the performance of all employees through a formal, annual performance evaluation.	Inspected a sample of employee annual review conversation reports to determine that the company evaluates the performance of all employees through a formal performance evaluation at least annually.	No exceptions noted.

CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Keytos Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.	Inspected the Data Protection Policy to determine that the policy documents how customer data may be made accessible and should be handled. Observed records of the Data Protection Policy to determine that all relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Keytos has an established policy and procedures that governs the use of cryptographic controls.	Inspected the Encryption Policy to determine that the company is required to implement authorized cryptographic controls and key protection procedures to protect individual systems and information.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Keytos 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.	Inspected the Microsoft Azure security center showing compliance with the regulatory standards to determine that control self-assessments are conducted. Inspected the Information Security Policy to determine that the company requires monitoring activities to be conducted on an ongoing basis or on a random basis whenever deemed necessary.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Keytos conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Microsoft Azure security center showing compliance with the regulatory standards to determine that continuous control monitoring is in place. Inspected the Information Security Policy to determine that the company requires monitoring activities to be conducted on an ongoing basis or on a random basis whenever deemed necessary.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information	Keytos conducts a Risk Assessment at least annually.	Inspected a sample of annual risk assessments reports detailing risk assessment approach, risk score matrix, results, and treatment plan	No exceptions noted.

	to support the functioning of internal control.		to determine that the company conducts annual risk assessments. Inspected the Risk Assessment Policy to determine that the company's risk assessment report is required to be updated when newly identified risks are identified and that the report should be updated and reviewed at least once per year.	
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Keytos has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inspected the Information Security Policy to determine that the policy covers processes and procedures to support the functioning of internal control. Observed records of the Information Security Policy to determine that all relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Keytos authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	Inspected the System Access Control Policy to determine that the company grants users access to company systems and applications based on the least-access principle.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Keytos identifies, inventories, classifies, and assigns owners to IT assets.	Inspected a list of the company's digital assets inventoried by CloudWatcher to determine that the company uses CloudWatcher to maintain an inventory of its digital assets. Inspected the asset inventory which includes physical and virtual assets along with their descriptions and owners to determine that the company maintains an asset inventory. Inspected the Asset Management Policy to determine that the company has documented the standards for maintaining an asset inventory for physical and virtual assets.	No exceptions noted.

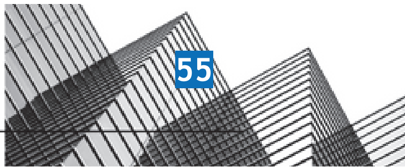
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Keytos maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control.	Inspected the company's architectural diagram which shows network components and workflow to determine that an accurate architectural diagram is maintained. Inspected the Asset Management Policy to determine that a network diagram is available to all appropriate service personnel and is kept current.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Keytos has established a Data Protection Policy and requires all employees to accept it upon hire. Management monitors employees' acceptance of the policy.	Inspected the Data Protection Policy to determine that the company has established a Data Protection Policy. Observed records of policy to determine that most of the relevant employees have accepted the policy.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Keytos provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	Inspected the Responsible Disclosure Policy to determine that the company provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, concerns, and other complaints to company management.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Keytos has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the policy includes creating, prioritizing, assigning, and tracking follow-ups to completion. Observed a list of all vulnerabilities detected in GitHub code to determine that the company has implemented procedures to track, prioritize, assign, and follow up to the completion of the incidents.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support	Keytos has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to	Inspected the Incident Response Plan to determine that the policy outlines management responsibilities and procedures to ensure a quick, effective, and/or orderly response to information security incidents and annual testing.	No exceptions noted.

	the functioning of internal control.	information security incidents and annual testing.	Observed records of the Incident Response Plan to determine that all the relevant employees have accepted the policy and that the policy has been approved within the last year.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Keytos conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Microsoft Azure security center showing compliance with the regulatory standards to determine that continuous control monitoring is in place. Inspected the Information Security Policy to determine that the company requires monitoring activities to be conducted on an ongoing basis or on a random basis whenever deemed necessary.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Keytos Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected the personnel data to determine that all policies have been approved by the management and that current employees and contractors have accepted the policies. Inspected the Information Security Policy to determine that all ISP policies are required to be reviewed, modified, or edited by management annually and accessible to employees.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The security team communicates important information security events to company management in a timely manner.	Inspected the Incident Response Plan to determine that the company requires users to report any incidents to the immediate manager within 24 hours, and the managers are required to notify the ISM. Disclosure: No security incidents have occurred during the audit period.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control,	Keytos has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Keytos's security	Inspected the Information Security Policy to determine that the company requires all new hires to complete information security awareness training as part of the onboarding process and annually thereafter.	No exceptions noted.

	necessary to support the functioning of internal control.	policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.		
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Keytos has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Observed that the company has designated Igal Flegmann as the person responsible for incident response at Keytos. Inspected the Incident Response Plan to determine that the company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Keytos has implemented an Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the Information Security Manager is required to conduct a post-mortem that includes a root cause analysis and documentation of any lessons learned after an incident has been resolved. Disclosure: No incidents occurred during the observation period.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Keytos has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	Inspected the Code of Conduct to determine that the company has defined the ethical standards that all personnel are required to follow while performing their duties. Additionally reviewed the policy acknowledgment data to determine that all employees have accepted the company Policies including the Code of Conduct.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities	Keytos has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the	Inspected the Acceptable Use Policy, which specifies the acceptable use of end-user computing devices and technology, to determine that the company has policies and procedures	No exceptions noted.

	for internal control, necessary to support the functioning of internal control.	company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire.	in place to establish acceptable use of information assets. Additionally reviewed the policy acknowledgment data to determine that all employees have accepted the company's Acceptable Use Policy.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the vendor details to determine that the company manages its vendors on Drata including their risk levels and compliance reports. Inspected the Vendor Management Policy to determine that the company retains the prerogative to conduct audits of its IT vendors and partners.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the vendor details to determine that the company maintains a vendor directory on Drata along with their risk levels and links to their Terms of Service and Privacy Policy. Inspected the Vendor Management Policy to determine that the company is required to maintain a vendor inventory and vendor contracts that address relevant security and privacy commitments.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Keytos has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the policy outlines management responsibilities and procedures to ensure a quick, effective, and/or orderly response to information security incidents and annual testing. Observed records of the Incident Response Plan to determine that all the relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters	Keytos has identified an incident response team that quantifies and monitors incidents involving security,	Observed that the company has designated Igal Flegmann as the person responsible for incident response at Keytos.	No exceptions noted.

	affecting the functioning of internal control.	availability, processing integrity, and confidentiality at the company.	Inspected the Incident Response Plan to determine that the company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Keytos tracks security deficiencies through internal tools and closes them within an SLA that management has pre-specified.	Observed that the identified vulnerabilities are tracked. Inspected the Vulnerability Management Policy to determine that the company has defined priority/severity ratings and SLAs to address critical, high, medium, and low priority level vulnerabilities.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Keytos communicates system changes to customers that may affect security, availability, processing integrity, or confidentiality.	Observed a newsletter sent to the customer via email, stating the new features introduced by the company to determine that the company communicates system changes to customers that may affect security, availability, processing integrity, or confidentiality.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Keytos has implemented an Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the Information Security Manager is required to conduct a post-mortem that includes a root cause analysis and documentation of any lessons learned after an incident has been resolved. Disclosure: No incidents occurred during the observation period.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Keytos has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the policy includes creating, prioritizing, assigning, and tracking follow-ups to completion. Observed a list of all vulnerabilities detected in GitHub code to determine that the company has implemented procedures to track,	No exceptions noted.



			prioritize, assign, and follow up to the completion of the incidents.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Keytos maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	Inspected the Privacy Policy on the company's website to determine that the company communicates its commitments regarding security and privacy through the publicly available Privacy Policy.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Keytos maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Client Agreements or Master Service Agreements are in place for when the Terms of Service may not apply.	Inspected the Terms of Use on the company's website to determine that the company communicates the service terms through the Terms of Use.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Keytos provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	Inspected the Responsible Disclosure Policy to determine that the company provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints. Observed a contact us page available on the company's website to determine that the company provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Keytos's security commitments are communicated to external users, as appropriate.	Inspected the company's Terms of Use and Privacy Policy, which detail the company's data security and protection measures to determine that security commitments are communicated to external users through the company's website.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the	Keytos has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for	No exceptions noted.

	identification and assessment of risks relating to objectives.	based on identified threats and the specified tolerances.	identified risks based on their severity levels.	
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Keytos conducts a Risk Assessment at least annually.	Inspected a sample of annual risk assessments reports detailing risk assessment approach, risk score matrix, results, and treatment plan to determine that the company conducts annual risk assessments. Inspected the Risk Assessment Policy to determine that the company's risk assessment report is required to be updated when newly identified risks are identified and that the report should be updated and reviewed at least once per year.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Keytos engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected an application penetration test report issued by Prescient Security to determine that the company engages with a third-party to conduct penetration tests of the production environment at least annually. Inspected the Vulnerability Management Policy to determine that penetration testing is required to be performed regularly by a penetration tester on Keytos's security team or an independent third party.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Keytos engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the quarterly code scans in GitHub to determine that quarterly vulnerability scans are performed at the company. Inspected the Vulnerability Management Policy to determine that the company requires all production systems to be scanned for vulnerabilities at least quarterly	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its	Keytos maintains a directory of its key vendors, including their compliance reports. Critical	Inspected the vendor details to determine that the company manages its vendors on Drata including their	No exceptions noted.

	objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	vendor compliance reports are reviewed annually.	risk levels and compliance reports. Inspected the Vendor Management Policy to determine that the company retains the prerogative to conduct audits of its IT vendors and partners.	
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Keytos engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the quarterly code scans in GitHub to determine that quarterly vulnerability scans are performed at the company. Inspected the Vulnerability Management Policy to determine that the company requires all production systems to be scanned for vulnerabilities at least quarterly	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the vendor details to determine that the company maintains a vendor directory on Drata along with their risk levels and links to their Terms of Service and Privacy Policy. Inspected the Vendor Management Policy to determine that the company is required to maintain a vendor inventory and vendor contracts that address relevant security and privacy commitments.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Keytos conducts a Risk Assessment at least annually.	Inspected a sample of annual risk assessments reports detailing risk assessment approach, risk score matrix, results, and treatment plan to determine that the company conducts annual risk assessments. Inspected the Risk Assessment Policy to determine that the company's risk assessment report is required to be updated when newly identified risks are identified and that the report should be updated and reviewed at least once per year.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its	Keytos has defined a formal risk management process that specifies risk tolerances and the	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes	No exceptions noted.

	objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	process for evaluating risks based on identified threats and the specified tolerances.	and remediation strategies for identified risks based on their severity levels.	
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the annual risk assessment reports which contain a risk assessment approach, risk assessment results including a remediation plan, and risk register questions to determine that the company has prepared a remediation plan. Inspected the Risk Assessment Policy to determine that the company has established a risk remediation process that is required to be implemented to resolve incidents.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the annual risk assessment reports which contain a risk assessment approach, risk assessment results including a remediation plan, and risk register questions to determine that the company has prepared a remediation plan. Inspected the Risk Assessment Policy to determine that the company has established a risk remediation process that is required to be implemented to resolve incidents.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Keytos conducts a Risk Assessment at least annually.	Inspected a sample of annual risk assessments reports detailing risk assessment approach, risk score matrix, results, and treatment plan to determine that the company conducts annual risk assessments. Inspected the Risk Assessment Policy to determine that the company's risk assessment report is required to be updated when newly identified risks are identified and that the report should be updated and reviewed at least once per year.	No exceptions noted.

CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Keytos engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected an application penetration test report issued by Prescient Security to determine that the company engages with a third-party to conduct penetration tests of the production environment at least annually. Inspected the Vulnerability Management Policy to determine that penetration testing is required to be performed regularly by a penetration tester on Keytos's security team or an independent third party.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Keytos engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the quarterly code scans in GitHub to determine that quarterly vulnerability scans are performed at the company. Inspected the Vulnerability Management Policy to determine that the company requires all production systems to be scanned for vulnerabilities at least quarterly	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Keytos conducts a Risk Assessment at least annually.	Inspected a sample of annual risk assessments reports detailing risk assessment approach, risk score matrix, results, and treatment plan to determine that the company conducts annual risk assessments. Inspected the Risk Assessment Policy to determine that the company's risk assessment report is required to be updated when newly identified risks are identified and that the report should be updated and reviewed at least once per year.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Keytos reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Inspected the organization chart to determine that the company is headed by the CEO, and the Business Development and Head of Marketing report directly to the CEO.	No exceptions noted.

CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the vendor details to determine that the company maintains a vendor directory on Drata along with their risk levels and links to their Terms of Service and Privacy Policy. Inspected the Vendor Management Policy to determine that the company is required to maintain a vendor inventory and vendor contracts that address relevant security and privacy commitments.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Keytos engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected an application penetration test report issued by Prescient Security to determine that the company engages with a third-party to conduct penetration tests of the production environment at least annually. Inspected the Vulnerability Management Policy to determine that penetration testing is required to be performed regularly by a penetration tester on Keytos's security team or an independent third party.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Keytos performs annual access control reviews.	Inspected a list of employees along with their emails and access status for various accounts to determine that the company performs access control reviews at least annually. Inspected the System Access Control Policy to determine that all access to Keytos systems and services is reviewed and updated on a quarterly basis to ensure proper authorizations are in place commensurate with job functions.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to	Keytos conducts a Risk Assessment at least annually.	Inspected a sample of annual risk assessments reports detailing risk assessment approach, risk score matrix, results, and treatment plan to determine that the company	No exceptions noted.

	ascertain whether the components of internal control are present and functioning.		conducts annual risk assessments. Inspected the Risk Assessment Policy to determine that the company's risk assessment report is required to be updated when newly identified risks are identified and that the report should be updated and reviewed at least once per year.	
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the vendor details to determine that the company maintains a vendor directory on Drata along with their risk levels and links to their Terms of Service and Privacy Policy. Inspected the Vendor Management Policy to determine that the company is required to maintain a vendor inventory and vendor contracts that address relevant security and privacy commitments.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Keytos has a defined System Access Control Policy that requires annual access control reviews to be conducted and access request forms be filled out for new hires and employee transfers.	Inspected the System Access Control Policy to determine that the company requires access requests to be formally made by workforce members and approved by the Security Officer and access privileges to be reviewed and updated quarterly.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Keytos engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the quarterly code scans in GitHub to determine that quarterly vulnerability scans are performed at the company. Inspected the Vulnerability Management Policy to determine that the company requires all production systems to be scanned for vulnerabilities at least quarterly	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to	Keytos has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity,	Observed that the company has designated Igal Flegmann as the person responsible for incident response at Keytos.	No exceptions noted.

	those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	and confidentiality at the company.	Inspected the Incident Response Plan to determine that the company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Keytos engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected an application penetration test report issued by Prescient Security to determine that the company engages with a third-party to conduct penetration tests of the production environment at least annually. Inspected the Vulnerability Management Policy to determine that penetration testing is required to be performed regularly by a penetration tester on Keytos's security team or an independent third party.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Keytos has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the list of key personnel to determine that the company has designated a security committee comprising one member.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including	Keytos has implemented an Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the Information Security Manager is required to conduct a post-mortem that includes a root cause analysis and documentation of any lessons learned after an incident has been resolved.	No exceptions noted.

	senior management and the board of directors, as appropriate.		Disclosure: No incidents occurred during the observation period.	
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the vendor details to determine that the company maintains a vendor directory on Drata along with their risk levels and links to their Terms of Service and Privacy Policy. Inspected the Vendor Management Policy to determine that the company is required to maintain a vendor inventory and vendor contracts that address relevant security and privacy commitments.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Keytos has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the policy outlines management responsibilities and procedures to ensure a quick, effective, and/or orderly response to information security incidents and annual testing. Observed records of the Incident Response Plan to determine that all the relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the annual risk assessment reports which contain a risk assessment approach, risk assessment results including a remediation plan, and risk register questions to determine that the company has prepared a remediation plan. Inspected the Risk Assessment Policy to determine that the company has established a risk remediation process that is required to be implemented to resolve incidents.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control	Keytos has implemented an Incident Response Plan that includes creating, prioritizing,	Inspected the Incident Response Plan to determine that the policy includes creating, prioritizing, assigning, and	No exceptions noted.

	deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	tracking follow-ups to completion. Observed a list of all vulnerabilities detected in GitHub code to determine that the company has implemented procedures to track, prioritize, assign, and follow up to the completion of the incidents.	
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Keytos engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the quarterly code scans in GitHub to determine that quarterly vulnerability scans are performed at the company. Inspected the Vulnerability Management Policy to determine that the company requires all production systems to be scanned for vulnerabilities at least quarterly	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Keytos conducts a Risk Assessment at least annually.	Inspected a sample of annual risk assessments reports detailing risk assessment approach, risk score matrix, results, and treatment plan to determine that the company conducts annual risk assessments. Inspected the Risk Assessment Policy to determine that the company's risk assessment report is required to be updated when newly identified risks are identified and that the report should be updated and reviewed at least once per year.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Keytos has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their severity levels.	No exceptions noted.
CC5.1	The entity selects and develops control	Keytos engages with third-party to conduct penetration tests of	Inspected an application penetration test report issued by Prescient	No exceptions noted.

	activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Security to determine that the company engages with a third-party to conduct penetration tests of the production environment at least annually. Inspected the Vulnerability Management Policy to determine that penetration testing is required to be performed regularly by a penetration tester on Keytos's security team or an independent third party.	
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Keytos reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Inspected the organization chart to determine that the company is headed by the CEO, and the Business Development and Head of Marketing report directly to the CEO.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Keytos conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Microsoft Azure security center showing compliance with the regulatory standards to determine that continuous control monitoring is in place. Inspected the Information Security Policy to determine that the company requires monitoring activities to be conducted on an ongoing basis or on a random basis whenever deemed necessary.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Keytos has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the list of key personnel to determine that the company has designated a security committee comprising one member.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to	Keytos engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and	Inspected the quarterly code scans in GitHub to determine that quarterly vulnerability scans are performed at the company.	No exceptions noted.

	the achievement of objectives to acceptable levels.	high priority findings are tracked to resolution.	Inspected the Vulnerability Management Policy to determine that the company requires all production systems to be scanned for vulnerabilities at least quarterly	
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Keytos conducts a Risk Assessment at least annually.	Inspected a sample of annual risk assessments reports detailing risk assessment approach, risk score matrix, results, and treatment plan to determine that the company conducts annual risk assessments. Inspected the Risk Assessment Policy to determine that the company's risk assessment report is required to be updated when newly identified risks are identified and that the report should be updated and reviewed at least once per year.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the annual risk assessment reports which contain a risk assessment approach, risk assessment results including a remediation plan, and risk register questions to determine that the company has prepared a remediation plan. Inspected the Risk Assessment Policy to determine that the company has established a risk remediation process that is required to be implemented to resolve incidents.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Keytos has an established policy and procedures that governs the use of cryptographic controls.	Inspected the Encryption Policy to determine that the company is required to implement authorized cryptographic controls and key protection procedures to protect individual systems and information.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the	Keytos engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected an application penetration test report issued by Prescient Security to determine that the company engages with a third-party to conduct penetration tests of the production environment at least annually.	No exceptions noted.

	achievement of objectives.		Inspected the Vulnerability Management Policy to determine that penetration testing is required to be performed regularly by a penetration tester on Keytos's security team or an independent third party.	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Keytos Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.	Inspected the Data Protection Policy to determine that the policy documents how customer data may be made accessible and should be handled. Observed records of the Data Protection Policy to determine that all relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Keytos Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected the personnel data to determine that all policies have been approved by the management and that current employees and contractors have accepted the policies. Inspected the Information Security Policy to determine that all ISP policies are required to be reviewed, modified, or edited by management annually and accessible to employees.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Keytos has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the list of key personnel to determine that the company has designated a security committee comprising one member.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to	Keytos authorizes access to information resources, including data and the systems that store or process customer data, based	Inspected the System Access Control Policy to determine that the company grants users access to company systems and applications based on the least-access principle.	No exceptions noted.

	support the achievement of objectives.	on the principle of least privilege.		
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Keytos has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with Keytos's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	Inspected the Information Security Policy to determine that the company requires all new hires to complete information security awareness training as part of the onboarding process and annually thereafter.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Keytos engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the quarterly code scans in GitHub to determine that quarterly vulnerability scans are performed at the company. Inspected the Vulnerability Management Policy to determine that the company requires all production systems to be scanned for vulnerabilities at least quarterly	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the annual risk assessment reports which contain a risk assessment approach, risk assessment results including a remediation plan, and risk register questions to determine that the company has prepared a remediation plan. Inspected the Risk Assessment Policy to determine that the company has established a risk remediation process that is required to be implemented to resolve incidents.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Keytos conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Microsoft Azure security center showing compliance with the regulatory standards to determine that continuous control monitoring is in place. Inspected the Information Security Policy to determine that the company	No exceptions noted.

			requires monitoring activities to be conducted on an ongoing basis or on a random basis whenever deemed necessary.	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Keytos conducts a Risk Assessment at least annually.	Inspected a sample of annual risk assessments reports detailing risk assessment approach, risk score matrix, results, and treatment plan to determine that the company conducts annual risk assessments. Inspected the Risk Assessment Policy to determine that the company's risk assessment report is required to be updated when newly identified risks are identified and that the report should be updated and reviewed at least once per year.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Keytos has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that the policy outlines the roles and responsibilities of the CEO and detailed procedures for the recovery of systems. Observed records of the Disaster Recovery Plan to determine that all relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Keytos has a formal Code of Conduct approved by management and accessible to all employees. All employees must accept the Code of Conduct upon hire.	Inspected the Code of Conduct to determine that the company has defined the ethical standards that all personnel are required to follow while performing their duties. Additionally reviewed the policy acknowledgment data to determine that all employees have accepted the company Policies including the Code of Conduct.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in	Keytos has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inspected the Information Security Policy to determine that the policy covers processes and procedures to support the functioning of internal control.	No exceptions noted.

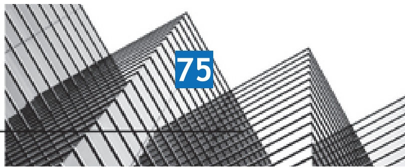
	procedures that put policies into action.		Observed records of the Information Security Policy to determine that all relevant employees have accepted the policy and that the policy has been approved within the last year.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Keytos conducts annual BCP/DR tests and documents according to the BCDR Plan.	Inspected a disaster recovery tabletop exercise report to determine that the conducts annual BCP/DR tests and documents according to the BCDR Plan. Inspected the Business Continuity and Disaster Recovery Plans to determine that both plans are required to be tested annually through simulations, tabletop, and technical testing.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Keytos has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the company has defined risk assessment processes and remediation strategies for identified risks based on their severity levels.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Management reviews security policies on an annual basis.	Inspected the policy list to determine that the Information Security Policy, Acceptable Use Policy, Physical Security Policy, Asset Management Policy, Incident Response Plan, System Access Control Policy, Encryption Policy, Data Protection Policy, and other security policies have been reviewed and approved on August 29, 2022. Inspected the Information Security Policy to determine that the company requires all ISPs to be reviewed, modified, and/or edited to meet necessary security standards.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Keytos Management has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible	Inspected the personnel data to determine that all policies have been approved by the management and that current employees and contractors have accepted the policies.	No exceptions noted.

		to all employees and contractors.	Inspected the Information Security Policy to determine that all ISP policies are required to be reviewed, modified, or edited by management annually and accessible to employees.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Keytos provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, and other complaints to company management.	Inspected the Responsible Disclosure Policy to determine that the company provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, concerns, and other complaints to company management.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Keytos has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	Inspected the Password Policy to determine that formal guidelines and requirements regarding password length and complexity, user authentication, and password protection have been established by the management.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Keytos requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.	Observed that all GitHub and Azure accounts have MFA enabled. Inspected the personnel directory to determine that all current employees have MFA enabled on their devices. Inspected the Password Policy to determine that the company requires MFA to be enabled for all systems that provide the option for MFA.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them	Role-based security is in place for internal and external users, including super admin users.	Inspected the list of roles assigned along with their name, scope and condition to determine that role base security is implemented by the company. Inspected the System Access Control Policy to determine that the company requires users to be granted access to	No exceptions noted.

	from security events to meet the entity's objectives.		the organization's information systems based on their job responsibilities.	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Keytos ensures that a password manager is installed on all company-issued laptops.	Inspected the personnel directory to determine that all current employees have password managers installed on their devices. Inspected the Password Policy to determine that the company requires all employees to use the approved password manager, BitWarden on their workstations to store their passwords electronically.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Keytos maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.	Inspected the company's network diagram showing the firewall rules and databases to determine that the company maintains an accurate network diagram. Inspected the CloudWatcher baseline configurations documentation showing the firewall rules and resource groups to determine that the company has restricted access to its IPs. Inspected the Asset Management Policy to determine that the company is required to maintain a network diagram, and is required to provide it to all appropriate service personnel.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Keytos has an established key management process in place to support the organization's use of cryptographic techniques.	Inspected the Encryption Policy to determine that the company has defined a process for key management and requires keys to be managed using software that automatically manages the key generation, access control, secure storage, backup, and rotation of keys.	No exceptions noted.

CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Keytos identifies, inventories, classifies, and assigns owners to IT assets.	Inspected a list of the company's digital assets inventoried by CloudWatcher to determine that the company uses CloudWatcher to maintain an inventory of its digital assets. Inspected the asset inventory which includes physical and virtual assets along with their descriptions and owners to determine that the company maintains an asset inventory. Inspected the Asset Management Policy to determine that the company has documented the standards for maintaining an asset inventory for physical and virtual assets.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Keytos stores customer data in databases that is encrypted at rest.	Inspected the Data Protection Policy to determine that the company stores customer data in databases that are encrypted at rest. Observed records of Azure showing that Microsoft Azure provides encryption at rest to determine that the company stores customer data in databases that are encrypted at rest.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Keytos ensures that company-issued laptops have encrypted hard-disks.	Inspected the Information Security Policy to determine that the company ensures that company-issued laptops have encrypted hard disks. Observed a list of personnel records showing that all relevant employees have hard disk encryption enabled to determine that the company ensures that company-issued laptops have encrypted hard disks.	No exceptions noted.
CC6.1	The entity implements logical access security software,	Access to corporate network, production machines, network devices, and support tools requires a unique ID.	Observed that employees have unique Office 365 accounts to determine that unique accounts are utilized.	No exceptions noted.

	infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		Inspected the System Access Control Policy to determine that users are required to use unique user IDs and passwords to access systems and applications.	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Hardening standards are in place to ensure that newly deployed server instances are appropriately secured.	Inspected the Asset Management Policy to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured. Observed a CloudWatcher Baseline configuration to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Keytos uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	Observed that the company uses GitHub as its version control system and only authorized personnel can access and change the code in GitHub. Inspected the Software Development Life Cycle to determine that the company is required to use a configuration control system.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users.	Inspected details of the MFA policy in Azure which is enabled, to determine that authentication protocols to authenticate into application are implemented. Inspected the Password Policy to determine that complex passwords are required to be used where possible, which have at least 10 characters, including uppercase and lowercase letters and non-alphanumeric characters.	No exceptions noted.



CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.	Inspected the new employee dashboard displaying access enabled and offboarding checklist to determine that a process is in place to grant appropriate access privileges to employees based on their job requirements. Inspected the System Access Control Policy to determine that the company requires access requests to be made by members and approved by Security Officer to the extent necessary for the requestor's job functions.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Access to corporate network, production machines, network devices, and support tools requires a unique ID.	Observed that employees have unique Office 365 accounts to determine that unique accounts are utilized. Inspected the System Access Control Policy to determine that users are required to use unique user IDs and passwords to access systems and applications.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by	Keytos performs annual access control reviews.	Inspected a list of employees along with their emails and access status for various accounts to determine that the company performs access control reviews at least annually. Inspected the System Access Control Policy to determine that all access to Keytos systems and services is reviewed and updated on a quarterly basis to ensure proper authorizations are in place commensurate with job functions.	No exceptions noted.

	the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Access to infrastructure and code review tools is removed from terminated employees within one business day.	Inspected the personnel directory to determine that all GitHub accounts linked to removed users are removed properly. Inspected the System Access Control Policy to determine that the Security Officer is required to terminate users' access rights within 1 business day of termination.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	External users must accept the Terms of Service prior to their account being created.	Inspected the company's application installation window which requires users to accept the License Agreement terms prior to installation to determine that external users are required to accept the service terms before using the company's services.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new	Keytos uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization	Inspected the offboarding checklist displaying removed access to determine that the company uses a checklist to revoke access of employees who leave the company.	No exceptions noted.

	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.	assets (physical or electronic) are properly returned.	Inspected the System Access Control Policy, which states that the HR department, users, and their supervisors are required to facilitate the Security Officer for the completion of the termination checklist.	
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Keytos has a defined System Access Control Policy that requires annual access control reviews to be conducted and access request forms be filled out for new hires and employee transfers.	Inspected the System Access Control Policy to determine that the company requires access requests to be formally made by workforce members and approved by the Security Officer and access privileges to be reviewed and updated quarterly.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.	Inspected the new employee dashboard displaying access enabled and offboarding checklist to determine that a process is in place to grant appropriate access privileges to employees based on their job requirements. Inspected the System Access Control Policy to determine that the company requires access requests to be made by members and approved by Security Officer to the extent necessary for the requestor's job functions.	No exceptions noted.

	user access is no longer authorized.			
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives.	Appropriate levels of access to infrastructure and code review tools are granted to new employees within one week of their start date.	Inspected the new employee dashboard displaying access enabled and offboarding checklist to determine that a process is in place to grant appropriate access privileges to employees based on their job requirements. Inspected the System Access Control Policy to determine that the company requires access requests to be made by members and approved by Security Officer to the extent necessary for the requestor's job functions.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives.	Keytos performs annual access control reviews.	Inspected a list of employees along with their emails and access status for various accounts to determine that the company performs access control reviews at least annually. Inspected the System Access Control Policy to determine that all access to Keytos systems and services is reviewed and updated on a quarterly basis to ensure proper authorizations are in place commensurate with job functions.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles,	Role-based security is in place for internal and external users, including super admin users.	Inspected the list of roles assigned along with their name, scope and condition to determine that role base security is implemented by the company. Inspected the System Access Control Policy to determine that the company requires users to be granted access to	No exceptions noted.

	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 organization's information systems based on their job responsibilities.	
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Keytos uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.	Inspected the offboarding checklist displaying removed access to determine that the company uses a checklist to revoke access of employees who leave the company. Inspected the System Access Control Policy, which states that the HR department, users, and their supervisors are required to facilitate the Security Officer for the completion of the termination checklist.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Access to corporate network, production machines, network devices, and support tools requires a unique ID.	Observed that employees have unique Office 365 accounts to determine that unique accounts are utilized. Inspected the System Access Control Policy to determine that users are required to use unique user IDs and passwords to access systems and applications.	No exceptions noted.
CC6.3	The entity authorizes,	Access to infrastructure and code review tools is removed	Inspected the personnel directory to determine that all GitHub accounts	No exceptions noted.

	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.	from terminated employees within one business day.	linked to removed users are removed properly. Inspected the System Access Control Policy to determine that the Security Officer is required to terminate users' access rights within 1 business day of termination.	
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Keytos has a defined System Access Control Policy that requires annual access control reviews to be conducted and access request forms be filled out for new hires and employee transfers.	Inspected the System Access Control Policy to determine that the company requires access requests to be formally made by workforce members and approved by the Security Officer and access privileges to be reviewed and updated quarterly.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the	External users must accept the Terms of Service prior to their account being created.	Inspected the company's application installation window which requires users to accept the License Agreement terms prior to installation to determine that external users are required to accept the service terms before using the company's services.	No exceptions noted.

	concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the vendor details to determine that the company maintains a vendor directory on Drata along with their risk levels and links to their Terms of Service and Privacy Policy. Inspected the Vendor Management Policy to determine that the company is required to maintain a vendor inventory and vendor contracts that address relevant security and privacy commitments.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Keytos has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors.	Inspected the Physical Security Policy stating the access requirements and building standards for asset security to determine that the company has established and approved a Physical Security Policy.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the vendor details to determine that the company manages its vendors on Drata including their risk levels and compliance reports. Inspected the Vendor Management Policy to determine that the company retains the prerogative to conduct audits of its IT vendors and partners.	No exceptions noted.

CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Keytos performs annual access control reviews.	Inspected a list of employees along with their emails and access status for various accounts to determine that the company performs access control reviews at least annually. Inspected the System Access Control Policy to determine that all access to Keytos systems and services is reviewed and updated on a quarterly basis to ensure proper authorizations are in place commensurate with job functions.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Keytos uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned.	Inspected the offboarding checklist displaying removed access to determine that the company uses a checklist to revoke access of employees who leave the company. Inspected the System Access Control Policy, which states that the HR department, users, and their supervisors are required to facilitate the Security Officer for the completion of the termination checklist.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Keytos has security policies that have been approved by management and detail how physical security for the company's headquarters is maintained. These policies are accessible to all employees and contractors.	Inspected the Physical Security Policy to determine that the physical security of data centers is ensured by the company's cloud infrastructure service provider.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only	Keytos uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified	Inspected the offboarding checklist displaying removed access to determine that the company uses a checklist to revoke access of employees who leave the company.	No exceptions noted.

	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.	timeframe and all organization assets (physical or electronic) are properly returned.	Inspected the System Access Control Policy, which states that the HR department, users, and their supervisors are required to facilitate the Security Officer for the completion of the termination checklist.	
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Keytos has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	Inspected the Asset Management Policy to determine that the company has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Keytos ensures that all company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.	Inspected the device compliance data to determine that all employees have screensaver lock enabled. Inspected the System Access Control Policy to determine that the company requires users to make information systems inaccessible by any other individual by using a password-protected screen saver or logging off when left unattended.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Keytos ensures that all connections to its web application from its users are encrypted.	Observed that SSL/TLS enforced to determine that all connections to its web application from its users are encrypted. Inspected the Data Protection Policy to determine that the company requires all Internet and intranet connections to be encrypted and authenticated using a strong protocol, key exchange, and cipher.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect	SSH users use unique accounts to access production machines. Additionally, the use of the "Root" account is not allowed.	Inspected the System Access Control Policy to determine that the company requires default accounts on all production systems, including root,	No exceptions noted.

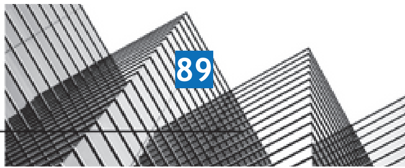
	against threats from sources outside its system boundaries.		to be disabled. Moreover, access to the systems and applications requires unique user login IDs and passwords for each individual user and developer.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	WAF in place to protect Keytos's application from outside threats.	Inspected the dashboard displaying overview to determine to protect applications from outside threats. Inspected the System Access Control Policy to determine that the company requires all workstations to have firewalls enabled to prevent unauthorized access unless explicitly granted.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Inspected the Data Protection Policy to determine that an intrusion detection system (IDS) is in place to detect potential intrusions, and alert personnel when a potential intrusion is detected. Observed CloudWatcher configuration data and Microsoft Defender dashboard showing monitoring results to determine that an intrusion detection system (IDS) is in place to detect potential intrusions and is configured to alert personnel when a potential intrusion is detected.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Keytos has established formal guidelines for passwords to govern the management and use of authentication mechanisms.	Inspected the Password Policy to determine that formal guidelines and requirements regarding password length and complexity, user authentication, and password protection have been established by the management.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Read/Write access to cloud data storage is configured to restrict public access.	Observed that all existing Azure buckets are private to determine that read/write access to cloud data storage is configured to restrict public access. Inspected the System Access Control Policy to determine that the level of security assigned to a user of the organization's information systems is	No exceptions noted.

			based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Keytos automatically logs users out after a predefined inactivity interval and/or closure of the internet browser, and requires users to reauthenticate	Inspected the System Access Control Policy to determine that the company automatically logs users out after a predefined inactivity interval and/or closure of the internet browser, and requires users to re-authenticate. Observed a user login page of the company's portal which requires authentication every time the user opens the browser tab to determine that configurations are in place to automatically log users out after a predefined inactivity interval and/or closure of the internet browser, and requires users to authenticate.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Keytos maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.	Inspected the company's network diagram showing the firewall rules and databases to determine that the company maintains an accurate network diagram. Inspected the CloudWatcher baseline configurations documentation showing the firewall rules and resource groups to determine that the company has restricted access to its IPs. Inspected the Asset Management Policy to determine that the company is required to maintain a network diagram, and is required to provide it to all appropriate service personnel.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Username and password (password standard implemented) or SSO required to authenticate into application, MFA optional for external users, and MFA required for employee users.	Inspected details of the MFA policy in Azure which is enabled, to determine that authentication protocols to authenticate into application are implemented. Inspected the Password Policy to determine that complex passwords	No exceptions noted.

			are required to be used where possible, which have at least 10 characters, including uppercase and lowercase letters and non-alphanumeric characters.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Keytos requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.	Observed that all GitHub and Azure accounts have MFA enabled. Inspected the personnel directory to determine that all current employees have MFA enabled on their devices. Inspected the Password Policy to determine that the company requires MFA to be enabled for all systems that provide the option for MFA.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Keytos uses configurations that ensure only approved networking ports and protocols are implemented, including firewalls.	Inspected the Asset Management Policy to determine that the company requires insecure and unnecessary communication protocols to be disabled. Observed a Cloudwatcher baseline configuration that includes firewall rules to determine that the company uses configurations that ensure only approved networking ports and protocols are implemented, including firewalls.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Keytos ensures that all connections to its web application from its users are encrypted.	Observed that SSL/TLS enforced to determine that all connections to its web application from its users are encrypted. Inspected the Data Protection Policy to determine that the company requires all Internet and intranet connections to be encrypted and authenticated using a strong protocol, key exchange, and cipher.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of	Keytos ensures that company-issued laptops have encrypted hard-disks.	Inspected the Information Security Policy to determine that the company ensures that company-issued laptops have encrypted hard disks.	No exceptions noted.

	information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.		Observed a list of personnel records showing that all relevant employees have hard disk encryption enabled to determine that the company ensures that company-issued laptops have encrypted hard disks.	
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Keytos stores customer data in databases that is encrypted at rest.	Inspected the Data Protection Policy to determine that the company stores customer data in databases that are encrypted at rest. Observed records of Azure showing that Microsoft Azure provides encryption at rest to determine that the company stores customer data in databases that are encrypted at rest.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Keytos's customer data is segregated from the data of other customers	Inspected the Data Protection Policy to determine that the company's customer data is to be segregated from the data of other customers Observed a list of customer tenant ids and subscription ids, a list of test data, and production data to determine that the company's customer data is segregated from the data of other customers.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or	Keytos uses DLP (Data Loss Prevention) software to prevent unencrypted sensitive information from being transmitted over email	Inspected the Information Security Policy to determine that the company uses DLP (Data Loss Prevention) software to prevent unencrypted sensitive information from being transmitted over email Observed Microsoft Purview DLP policy to determine that the company uses DLP (Data Loss Prevention) software to prevent unencrypted	No exceptions noted.

	removal to meet the entity's objectives.		sensitive information from being transmitted over email.	
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Keytos uses encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	Observed that the admin pages of AWS, Atlas, and Azure have SSL/TLS enabled. Inspected the Data Protection Policy to determine that the company requires all Internet and intranet connections to be encrypted.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	SSH users use unique accounts to access production machines. Additionally, the use of the "Root" account is not allowed.	Inspected the System Access Control Policy to determine that the company requires default accounts on all production systems, including root, to be disabled. Moreover, access to the systems and applications requires unique user login IDs and passwords for each individual user and developer.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Keytos requires antivirus software to be installed on workstations to protect the network against malware.	Inspected the personnel directory to determine that all current employees have anti-malware software installed on their workstations. Inspected the Asset Management Policy to determine that the company requires antivirus and anti-malware tools to be deployed on all end-point devices.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Keytos's workstations operating system (OS) security patches are applied automatically.	Inspected the personnel data to determine that automatic updates are enabled on all current employees' workstations. Inspected the Asset Management Policy to determine that the company is required to implement OS patches	No exceptions noted.



			periodically, in order of criticality, and during off-peak hours.	
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Keytos has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	Inspected the log analytics dashboard on Microsoft Azure showing a list of logs upon a query to determine that the company has infrastructure logging configured to monitor web traffic and suspicious activity. Inspected the alert rules in Microsoft Azure to determine that the company has enabled CloudWatcher to generate alerts upon detecting an anomaly. Inspected the Data Protection Policy to determine that the company is required to use Azure Monitor and CloudWatcher to monitor the entire cloud service operation, and if a system failure and alarm is triggered, key personnel are required to be notified by text, chat, and/or email message in order to take appropriate corrective action.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Keytos conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	Inspected the Microsoft Azure security center showing compliance with the regulatory standards to determine that continuous control monitoring is in place. Inspected the Information Security Policy to determine that the company requires monitoring activities to be conducted on an ongoing basis or on a random basis whenever deemed necessary.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations	Keytos engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected an application penetration test report issued by Prescient Security to determine that the company engages with a third-party to conduct penetration tests of the production environment at least annually.	No exceptions noted.

	that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		Inspected the Vulnerability Management Policy to determine that penetration testing is required to be performed regularly by a penetration tester on Keytos's security team or an independent third party.	
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Inspected the Data Protection Policy to determine that an intrusion detection system (IDS) is in place to detect potential intrusions, and alert personnel when a potential intrusion is detected. Observed CloudWatcher configuration data and Microsoft Defender dashboard showing monitoring results to determine that an intrusion detection system (IDS) is in place to detect potential intrusions and is configured to alert personnel when a potential intrusion is detected.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Keytos engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the quarterly code scans in GitHub to determine that quarterly vulnerability scans are performed at the company. Inspected the Vulnerability Management Policy to determine that the company requires all production systems to be scanned for vulnerabilities at least quarterly	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities	When Keytos's application code changes, code reviews and tests are performed by someone other than the person who made the code change.	Inspected a list of successful Code QL runs which are performed before pushing a code into repository to determine that the company has a code review process in place. Inspected the Software Development Life Cycle Policy to determine that the company requires all code changes to be reviewed by individuals in the executive team that are knowledgeable in code	No exceptions noted.

	to newly discovered vulnerabilities.		review techniques and secure coding practices.	
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Keytos uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	Observed that the company uses GitHub as its version control system and only authorized personnel can access and change the code in GitHub. Inspected the Software Development Life Cycle to determine that the company is required to use a configuration control system.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Keytos has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	Inspected the log analytics dashboard on Microsoft Azure showing a list of logs upon a query to determine that the company has infrastructure logging configured to monitor web traffic and suspicious activity. Inspected the alert rules in Microsoft Azure to determine that the company has enabled CloudWatcher to generate alerts upon detecting an anomaly. Inspected the Data Protection Policy to determine that the company is required to use Azure Monitor and CloudWatcher to monitor the entire cloud service operation, and if a system failure and alarm is triggered, key personnel are required to be notified by text, chat, and/or email message in order to take appropriate corrective action.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of	Keytos engages with third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and	Inspected the quarterly code scans in GitHub to determine that quarterly vulnerability scans are performed at the company. Inspected the Vulnerability	No exceptions noted.

	malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	high priority findings are tracked to resolution.	Management Policy to determine that the company requires all production systems to be scanned for vulnerabilities at least quarterly	
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected	Inspected the Data Protection Policy to determine that an intrusion detection system (IDS) is in place to detect potential intrusions, and alert personnel when a potential intrusion is detected. Observed CloudWatcher configuration data and Microsoft Defender dashboard showing monitoring results to determine that an intrusion detection system (IDS) is in place to detect potential intrusions and is configured to alert personnel when a potential intrusion is detected.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Keytos uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.	Inspected the log analytics dashboard on Microsoft Azure showing a list of logs upon a query to determine that the company uses a centralized logging system. Inspected the alert rules in Microsoft Azure to determine that the company has enabled CloudWatcher to generate alerts upon detecting an anomaly. Inspected the Asset Management Policy to determine that the company requires logging to be enabled on all systems as part of its system hardening standards.	No exceptions noted.
CC7.2	The entity monitors system components	Keytos is using Drata to monitor the security and compliance of	Observed that Azure infrastructure is linked to Drata to determine that the	No exceptions noted.

	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.	its cloud infrastructure configuration	company uses Drata to monitor the security and compliance of its cloud infrastructure configuration. Inspected the Asset Management Policy, Vulnerability Management Policy, and Information Security Policy, which state that the company uses Drata to maintain asset inventories, upload and maintain information security policies, and perform vulnerability scanning on workstations, to determine that the company uses Drata to monitor the security and compliance of its cloud infrastructure configuration.	
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Keytos's cloud infrastructure is monitored through an operational audit system that sends alerts to appropriate personnel	Inspected the CloudWatcher alert rules to determine that the company uses CloudWatcher to monitor its cloud infrastructure. Inspected an email from Microsoft Azure notifying the company about a generated alert from Azure Monitor to determine that the company uses Azure Monitor to monitor its cloud infrastructure. Inspected the CloudWatcher baseline documentation showing a list of configured alert rules to determine that the company uses CloudWatcher to monitor its cloud infrastructure. Inspected the Data Protection Policy to determine that the company is required to use Azure Monitor and CloudWatcher to monitor the entire cloud service operation, and if a system failure and alarm is triggered, key personnel are required to be notified by text, chat, and/or email message in order to take appropriate corrective action.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of	Keytos uses a system that collects and stores server logs in a central location. The system	Inspected the log analytics dashboard on Microsoft Azure showing a list of logs upon a query to determine that	No exceptions noted.

	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.	can be queried in an ad hoc fashion by authorized users.	the company uses a centralized logging system that can be queried. Inspected the Asset Management Policy to determine that the company requires logging to be enabled on all devices and systems.	
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Keytos has infrastructure logging configured to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	Inspected the log analytics dashboard on Microsoft Azure showing a list of logs upon a query to determine that the company has infrastructure logging configured to monitor web traffic and suspicious activity. Inspected the alert rules in Microsoft Azure to determine that the company has enabled CloudWatcher to generate alerts upon detecting an anomaly. Inspected the Data Protection Policy to determine that the company is required to use Azure Monitor and CloudWatcher to monitor the entire cloud service operation, and if a system failure and alarm is triggered, key personnel are required to be notified by text, chat, and/or email message in order to take appropriate corrective action.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability	Keytos tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Observed that the company uses GitHub to track and prioritize security deficiencies. Inspected the Vulnerability Management Policy to determine that the company follows a simple vulnerability tracking process using GitHub.	No exceptions noted.

	to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Keytos has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the policy outlines management responsibilities and procedures to ensure a quick, effective, and/or orderly response to information security incidents and annual testing. Observed records of the Incident Response Plan to determine that all the relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Keytos has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the policy includes creating, prioritizing, assigning, and tracking follow-ups to completion. Observed a list of all vulnerabilities detected in GitHub code to determine that the company has implemented procedures to track, prioritize, assign, and follow up to the completion of the incidents.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Keytos has implemented an Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the Information Security Manager is required to conduct a post-mortem that includes a root cause analysis and documentation of any lessons learned after an incident has been resolved. Disclosure: No incidents occurred during the observation period.	No exceptions noted.
CC7.3	The entity evaluates security events to	The security team communicates important	Inspected the Incident Response Plan to determine that the company	No exceptions noted.

	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.	information security events to company management in a timely manner.	requires users to report any incidents to the immediate manager within 24 hours, and the managers are required to notify the ISM. Disclosure: No security incidents have occurred during the audit period.	
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Keytos has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Observed that the company has designated Igal Flegmann as the person responsible for incident response at Keytos. Inspected the Incident Response Plan to determine that the company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Keytos tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Observed that the company uses GitHub to track and prioritize security deficiencies. Inspected the Vulnerability Management Policy to determine that the company follows a simple vulnerability tracking process using GitHub.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Keytos has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the policy includes creating, prioritizing, assigning, and tracking follow-ups to completion. Observed a list of all vulnerabilities detected in GitHub code to determine that the company has implemented procedures to track, prioritize, assign, and follow up to the completion of the incidents.	No exceptions noted.

CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Keytos has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the policy outlines management responsibilities and procedures to ensure a quick, effective, and/or orderly response to information security incidents and annual testing. Observed records of the Incident Response Plan to determine that all the relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Keytos has implemented an Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the Information Security Manager is required to conduct a post-mortem that includes a root cause analysis and documentation of any lessons learned after an incident has been resolved. Disclosure: No incidents occurred during the observation period.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Keytos has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Observed that the company has designated Igal Flegmann as the person responsible for incident response at Keytos. Inspected the Incident Response Plan to determine that the company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate,	Keytos tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Observed that the company uses GitHub to track and prioritize security deficiencies. Inspected the Vulnerability Management Policy to determine that the company follows a simple	No exceptions noted.

	and communicate security incidents, as appropriate.		vulnerability tracking process using GitHub.	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Keytos has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the policy includes creating, prioritizing, assigning, and tracking follow-ups to completion. Observed a list of all vulnerabilities detected in GitHub code to determine that the company has implemented procedures to track, prioritize, assign, and follow up to the completion of the incidents.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Keytos tracks and prioritizes security deficiencies through internal tools according to their severity by an independent technical resource.	Observed that the company uses GitHub to track and prioritize security deficiencies. Inspected the Vulnerability Management Policy to determine that the company follows a simple vulnerability tracking process using GitHub.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Keytos has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the policy outlines management responsibilities and procedures to ensure a quick, effective, and/or orderly response to information security incidents and annual testing. Observed records of the Incident Response Plan to determine that all the relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Keytos ensures that incident response plan testing is performed on an annual basis.	Inspected a disaster recovery exercise report to determine that incident response plan testing is performed on an annual basis. Inspected the Incident Response Plan to determine that the incident response plan is tested annually.	No exceptions noted.
CC7.5	The entity identifies, develops,	Keytos has identified an incident response team that	Observed that the company has designated Igal Flegmann as the	No exceptions noted.

	and implements activities to recover from identified security incidents.	quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	person responsible for incident response at Keytos. Inspected the Incident Response Plan to determine that the company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Keytos has implemented an Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the Information Security Manager is required to conduct a post-mortem that includes a root cause analysis and documentation of any lessons learned after an incident has been resolved. Disclosure: No incidents occurred during the observation period.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Keytos performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	Inspected the Backup Policy to determine that the company is required to perform daily data backups using an automated process that backs up all data to a separate region in the same country. Observed records of Azure showing daily data backup are enabled to determine that the company performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and	Keytos uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system admin.	Observed that the company uses GitHub as its version control system and only authorized personnel can access and change the code in GitHub. Inspected the Software Development Life Cycle to determine that the company is required to use a configuration control system.	No exceptions noted.

	procedures to meet its objectives.			
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Keytos ensures that code changes are tested prior to deployment to ensure quality and security.	Inspected details of a test code before being deployed to test portal and then to production to determine that code changes are tested prior to deployment to ensure quality and security. Inspected the Software Development Life Cycle Policy to determine that the company requires all code changes to be reviewed by individuals in the executive team that are knowledgeable in code review techniques and secure coding practices.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inspected the Software Development Life Cycle Policy to determine that the company has defined the software development phases, the security control guidelines, and change control procedures.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Separate environments are used for testing and production for Keytos's application	Inspected the dashboard displaying request access to determine that separate environments are used for testing and production. Inspected the Software Development Life Cycle Policy to determine that the company requires application development activity to be separated from the production and test environments.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests,	Only authorized Keytos personnel can push or make changes to production code.	Inspected the company's branch protection rules in GitHub to determine that access to push changes is restricted to authorized personnel.	No exceptions noted.

	approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		Observed that only authorized personnel have access to merge code into the default branch for all linked GitHub repositories. Inspected the Software Development Lifecycle Policy to determine that the company requires all changes to production environments to strictly follow change control procedures, including human approval of all changes, granted by an authorized owner of that environment.	
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Keytos ensures that releases are approved by appropriate members of management prior to production release.	Inspected the summary of a change in GitHub showing that the change was approved before deployment to determine that the company ensures that releases are approved by appropriate members of management prior to production release. Inspected the Software Development Life Cycle to determine that the company requires all changes to production code to be approved by an authorized owner of that environment.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	When Keytos's application code changes, code reviews and tests are performed by someone other than the person who made the code change.	Inspected a list of successful Code QL runs which are performed before pushing a code into repository to determine that the company has a code review process in place. Inspected the Software Development Life Cycle Policy to determine that the company requires all code changes to be reviewed by individuals in the executive team that are knowledgeable in code review techniques and secure coding practices.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities	Keytos performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	Inspected the Backup Policy to determine that the company is required to perform daily data backups using an automated process	No exceptions noted.

	for risks arising from potential business disruptions.		that backs up all data to a separate region in the same country. Observed records of Azure showing daily data backup are enabled to determine that the company performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Keytos has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that the policy outlines the roles and responsibilities of the CEO and detailed procedures for the recovery of systems. Observed records of the Disaster Recovery Plan to determine that all relevant employees have accepted the policy and that the policy has been approved within the last year.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Keytos has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lend support to Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the policy includes creating, prioritizing, assigning, and tracking follow-ups to completion. Observed a list of all vulnerabilities detected in GitHub code to determine that the company has implemented procedures to track, prioritize, assign, and follow up to the completion of the incidents.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Keytos has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents and annual testing.	Inspected the Incident Response Plan to determine that the policy outlines management responsibilities and procedures to ensure a quick, effective, and/or orderly response to information security incidents and annual testing. Observed records of the Incident Response Plan to determine that all the relevant employees have accepted the policy and that the	No exceptions noted.

			policy has been approved within the last year.	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Keytos has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Observed that the company has designated Igal Flegmann as the person responsible for incident response at Keytos. Inspected the Incident Response Plan to determine that the company has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Keytos has implemented an Incident Response Plan that includes documenting “Lessons Learned” and "Root Cause Analysis" after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery.	Inspected the Incident Response Plan to determine that the Information Security Manager is required to conduct a post-mortem that includes a root cause analysis and documentation of any lessons learned after an incident has been resolved. Disclosure: No incidents occurred during the observation period.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Keytos utilizes multiple availability zones to replicate production data across different zones.	Inspected the company's database configurations showing that multi-region reads and writes are enabled to determine that multiple availability zones are utilized to replicate production data across different zones. Inspected the Backup Policy to determine that the company requires an automated process to back up all data to a separate region in the same country.	No exceptions noted.

CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected the vendor details to determine that the company maintains a vendor directory on Drata along with their risk levels and links to their Terms of Service and Privacy Policy. Inspected the Vendor Management Policy to determine that the company is required to maintain a vendor inventory and vendor contracts that address relevant security and privacy commitments.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the vendor details to determine that the company manages its vendors on Drata including their risk levels and compliance reports. Inspected the Vendor Management Policy to determine that the company retains the prerogative to conduct audits of its IT vendors and partners.	No exceptions noted.