Keytos LLC

SOC 2 TYPE II REPORT

Description of the Keytos System

Controls Relevant to **Security**

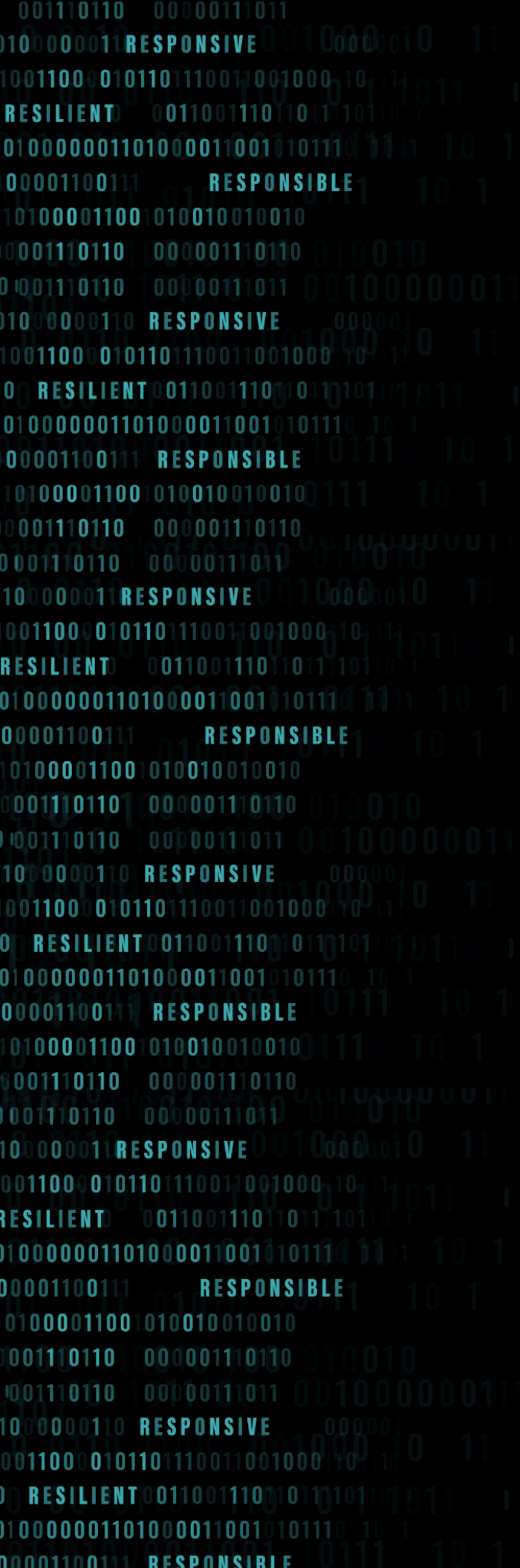
For Period 17 April 2024 to 16 April 2025

With Independent Service Auditor's Report
Including Tests Performed and Results Thereof

DECRYPT COMPLIANCE

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations

TABLE OF CONTENTS



SECTION I: MANAGEMENT ASSERTION

DECRYPT | COMPLIANCE

I. KEYTOS'S MANAGEMENT ASSERTION

We have prepared the accompanying description titled "Keytos's Description of the Keytos System" (Description) of Keytos LLC ("Service Organization") in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the Keytos (System) that may be useful when assessing the risks arising from interactions with the system throughout the period 17 April 2024 to 16 April 2025, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Complementary subservice organization controls:
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 controls. The Description does not disclose the actual controls at the subservice organization.

Complementary user entity controls:
The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Keytos LLC controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

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

a. The Description presents the System that was designed and implemented throughout the period 17 April 2024 to 16 April 2025 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary

user entity controls assumed in the design of Keytos LLC's controls throughout the period 17 April 2024 to 16 April 2025.

c. The Keytos LLC controls stated in the Description operated effectively throughout the period 17 April 2024 to 16 April 2025 to achieve the service commitments and system requirements based on the applicable trust services criteria, if user entities applied the complementary user entity controls assumed in the design of Keytos LLC's controls throughout the period 17 April 2024 to 16 April 2025.

Keytos LLC
July 2, 2025

SECTION II:
INDEPENDENT SERVICE AUDITOR'S REPORT

DECRYPT | COMPLIANCE

II. INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Keytos LLC:

Scope

We have examined Keytos LLC's (referred to hereafter as "Keytos LLC" or "the Company") accompanying "Keytos's Description of the Keytos System" for the passwordless authentication toolset services provided to user entities throughout the period 17 April 2024 to 16 April 2025 (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout the period 17 April 2024 to 16 April 2025 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Complementary subservice organization controls: 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 controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Complementary user entity controls: The Description also indicates that Keytos LLC's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Keytos LLC's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Other information provided by Keytos LLC

The information attached in the accompanying "SECTION V - Other Information Provided by Keytos" is presented by Keytos LLC to disclose, to the extent known, the causative factors for the deviations, the controls that mitigate the effect of the deviations, corrective actions taken, and other qualitative factors

that would assist users in understanding the effects of the deviations on the service organization's ability to achieve its service commitments and system requirements. Such information is not a part of the Keytos's Description of the Keytos System made available to user entities during the period 17 April 2024 to 16 April 2025. This information has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

Keytos LLC'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 the service commitments and system requirements were achieved. Keytos LLC has provided the accompanying assertion titled, "Keytos LLC's Management Assertion" (Assertion), about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Keytos LLC is responsible for (1) selecting the trust services criteria applicable to the Description; (2) preparing the Description and Assertion; (3) the completeness, accuracy, and method of presentation of the Description and Assertion; (4) providing the services covered by the Description; (5) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (6) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the Service Organization's service commitments and system requirements, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA"). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Performing procedures to obtain evidence about whether the controls stated in the Description are presented in accordance with the Description Criteria
- 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
- Assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively based on the applicable trust services criteria
- Testing the operating effectiveness of those controls based on the applicable trust services criteria
- 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 of Keytos LLC and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the *Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct* established by the AICPA. We have complied with such independence and other ethical requirements and applied the AICPA's Statements on Quality Management Standards.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs.

Because of their nature, controls at a service organization 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 evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls based on the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls we tested and the nature, timing, and results of those tests are listed in the accompanying "SECTION IV - Description of Criteria, Controls, Tests & Results of Tests" (Description of Tests and Results).

Opinion

In our opinion, in all material respects:

a. The Description presents the Keytos that was designed and implemented throughout the period 17 April 2024 to 16 April 2025 in accordance with the Description Criteria

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively and if user entities applied the controls assumed in the design of Keytos LLC's controls throughout the period 17 April 2024 to 16 April 2025
c. The controls stated in the Description operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period 17 April 2024 to 16 April 2025, if the user entity controls assumed in the design of Keytos LLC's controls operated effectively throughout the period 17 April 2024 to 16 April 2025

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Keytos LLC, user entities of the Keytos during some or all of the period 17 April 2024 to 16 April 2025 and prospective user entities, independent auditors and practitioners providing services to such user entities who have sufficient knowledge and understanding of the following:

- The nature of the services provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties, including complementary user entity controls assumed in the design of the service organization's controls
- Internal control and its limitations
- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- 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.

Decrypt Compliance PC

July 2, 2025
San Jose, CA

SECTION III:
KEYTOS' DESCRIPTION OF THE KEYTOS SYSTEM

III. KEYTOS'S DESCRIPTION OF THE KEYTOS SYSTEM

COMPANY & SYSTEM OVERVIEW AND BACKGROUND

Keytos LLC is a cybersecurity company specializing in Identity Management and PKI services, providing organizations with a seamless way to enhance security while reducing operational costs. Through our SaaS platform and expert resources, we eliminate the need for manual credential management by issuing short-term certificates for secure access to critical resources.

Founded in 2021, Keytos LLC serves 1,000+ customers worldwide, ranging from Fortune 500 companies to emerging startups. Our infrastructure is secured by robust security controls that have undergone SOC 2 and ISO 27001 audits, ensuring compliance and reliability.

Purpose and Scope of Report
The scope of this report is limited to the controls supporting Keytos and does not extend to other available software products and services or the controls at third-party service providers.

Products and Services offered
Keytos LLC offers a comprehensive suite of SaaS solutions, including UI, APIs, Plug-ins, and Managed Services:

Identity Management Services
Enabling organizations to extend corporate identity protections to SSH endpoints and GitHub accounts by issuing short-term SSH certificates. This approach provides just-in-time access without the need for traditional credentials.

PKI as a Service
A fully managed solution for SSL certificate management, empowering organizations to implement a passwordless authentication strategy with ease.

RADIUS as a Service (EZRADIUS)
A cloud-based RADIUS solution that complements our PKI services, providing a passwordless network authentication experience for Wi-Fi and VPN access.

Certificate Transparency Log Monitoring
Providing organizations with real-time visibility into all certificates issued for their domains. This proactive monitoring helps detect rogue certificates and prevent outages caused by expired certificates.

Passwordless Identity Onboarding

Simplifying the transition to passwordless authentication by managing the entire onboarding and lifecycle of passwordless credentials, reducing the risk of phishing attacks.

Keytos LLC is committed to securing digital identities and enabling organizations to adopt passwordless security strategies with confidence.

Organizational Structure

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.

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.

OVERVIEW OF THE COMPANY'S INTERNAL CONTROLS

Control Environment

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/ 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 Keytos toolset platform.

Authority and Responsibility

Board of Directors **-** The company's Board of Directors has a documented charter that outlines its oversight responsibilities for internal control and meets annually, demonstrating 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.

Management 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.

Human Resources Policy 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 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
- 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.

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.
- Security awareness training is completed by all Keytos LLC employees upon hire and annually thereafter.
- Employees are directed to report any potential security incidents to the IT Manager.
- Violations of Keytos LLC security policies have clearly defined repercussions.

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.

RISK ASSESSMENT

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.

Risk identification:

Keytos identifies, inventories, classifies, and assigns owners to IT assets. 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.

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 mitigation:
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.

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. Keytos maintains cybersecurity insurance to mitigate the financial impact of business disruptions. 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.

PENETRATION TESTING

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.

Control Activities

Information and Communication

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.

Internal communication

Keytos provides a channel to employees for reporting security incidents, and concerns, and other complaints to company management. Keytos maintains an architecture diagram to document system boundaries to support the functioning of internal control.

External communication

Keytos provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints. The following is communicated to external users:

- Keytos communicates system changes to customers that may affect security.
- Keytos maintains a Terms of Service that is available to external users and internal employees, and the terms detail the company's security commitments regarding the systems. Client agreements are in place for when the Terms of Service may not apply. External users are required to review and accept the Terms of Service prior to account creation, ensuring access is granted only to verified individuals who acknowledge and agree to the organization's usage and security requirements.
- Keytos maintains a Privacy Policy that is available to external users and internal employees, and it details the company's confidentiality and privacy commitments.

LOGICAL AND PHYSICAL ACCESS

SYSTEM ACCESS

Production Environment Logical Access

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.
- Keytos has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Strong password configuration settings, where applicable, are enabled, including:
  (1) Use a minimum of 8 characters
  (2) Use upper case, lower case, numeric, and special character values
  (3) Reuse prevention is limited to 24 versions
  (4) Multi factor authentication Phishing-resistant is enabled.

Termination of Access

Keytos maintains a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and organization assets (physical or electronic) are properly returned.

Physical Access and Visitors

Keytos LLC is a fully remote company with no centralized headquarters or physical network. There are specific considerations taken, however, regarding remote work and the security risks inherent specific to companies that are fully remote.

SOFTWARE DEVELOPMENT LIFECYCLE (SDLC) OVERVIEW

Keytos LLC's change management procedures are detailed in the Software Development Life Cycle Policy. The following requirements are implemented for all changes to the organization, business processes, information processing facilities, and systems that affect information security in Keytos LLC's production environment:

- 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.
- 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.
- Keytos's application code changes are reviewed by someone other than the person who made the code change prior to production deployment.
- Only authorized Keytos personnel can push or make changes to production code.

DESCRIPTION OF THE PRODUCTION ENVIRONMENT

Web, Application, and Service-Supporting Infrastructure Environment

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. Network security controls are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is

specifically denied. Additionally, a web application firewall and an intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected. Critical/high incidents are resolved timely.

Production Monitoring

Production systems and resources are monitored and automated alerts are sent out to personnel based on pre-configured rules.

SECURITY AND ARCHITECTURE

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. Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Changes to the baseline configuration standards are monitored to log and flag any anomalies.

Data Center Security

Keytos relies on the global infrastructure of Microsoft Azure which can include the facilities, network, hardware, and operational software that support the provisioning and use of basic computing resources and storage. This infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards and regulations.

The environmental protection managed by the vendors' policies are:

- ***Redundancy*** - The data centers are designed to anticipate and tolerate failure while maintaining service levels with core applications deployed to multiple regions.
- ***Fire Detection and Suppression*** – Automatic fire detection and suppression equipment have been installed to reduce risk.
- ***Redundant Power*** – the data center electrical power systems are designed to be fully redundant and maintainable without impact on operations, 24 hours a day, and Uninterruptible Power

Supply (UPS) units provide backup power in the event of an electrical failure. Data centers use generators to provide backup power for the entire facility.

- ***Climate and Temperature Controls*** – maintain a constant operating temperature and humidity level for all hardware.
- ***Physical access*** - Microsoft Azure recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures, and controls have been implemented to help prevent unauthorized access to data, assets, and restricted areas.

Infrastructure Security

- ***End-to-End Network Isolation*** - the Virtual Private Cloud is designed to be logically separated from other cloud customers and to prevent data within the cloud from being intercepted.
- ***External & Internal enforcement points*** - All servers are protected by restricted Microsoft Azure firewall rules. The configuration of the cloud providers' firewall rules is restricted to authorized personnel.
- ***Server Hardening*** - all servers are hardened according to industry best practices.

Application Security

- ***Penetration Testing*** - 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.
- ***Vulnerabilities Management*** - Keytos tracks and prioritizes security vulnerabilities weekly through internal tools according to severity. Critical/high vulnerabilities are remediated according to the vulnerability management policy.

Operational Security

- ***Security Incident Response Management*** - Keytos has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lending support to Business Continuity/Disaster Recovery. An incident response team that quantifies and monitors incidents involving security has been established. As part of the Incident Response Plan, documenting lessons learnt and root cause analysis after incidents and sharing them with the broader engineering team to support Business Continuity/Disaster Recovery is required. Keytos performs daily backups and retains them in accordance with a predefined schedule in the Backup Policy. A Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems has been established. Keytos conducts annual disaster recovery (DR) tests in alignment with its Disaster Recovery Plan. Test results are documented and reviewed to ensure recovery objectives are met and to support ongoing improvements to the plan.
- ***Endpoint Protection*** - Keytos ensures the following devices security controls to protect its digital assets and infrastructure:

- A screensaver lock with a timeout of no more than 15 minutes.
- Employees use a password manager to save, store, and organize passwords and logins in a personal vault protected on their devices.
- An antivirus software installed on workstations to protect the network against malware.
- An Operating System security patches are applied automatically on employees devices to reduce exposure to known vulnerabilities.
- Company-issued laptops have encrypted hard-disks.

Data Security

Keytos has established a comprehensive Data Protection Policy that employees are required to acknowledge upon hire, ensuring that all information assets are safeguarded through physical controls designed to prevent tampering, damage, theft, or unauthorized physical access. To further enhance data security, Keytos employs Data Loss Prevention (DLP) software configured to block the transmission of unencrypted sensitive information via email, thereby reducing the risk of data leakage and reinforcing the company's commitment to protecting confidential information. Customer data is segregated from the data of other customers to ensure privacy and isolation, and application user passwords are securely stored using a salted password hash to protect against unauthorized access and credential compromise.

- ***Data Encryption*** - Keytos has an established policy and procedures that governs the use of cryptographic controls.
- ***Data in Transit*** - Encryption on data in transit is enabled using a valid, authenticated HTTPS TLS 1.2 certificate, at minimum, to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.
- ***Data at Rest*** - Data at rest is encrypted using Transparent Data Encryption to ensure database files, transaction logs, and backups are encrypted using a database encryption key managed by a service-managed key.

Incident Management Process

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.

CHANGES TO THE SYSTEM AFTER THE EXAMINATION PERIOD

No significant changes have occurred to the services provided to user entities as of the date of this report.

SYSTEM INCIDENTS

No significant incidents have occurred to the service provided to user entities as of the date of this report.

COMPLEMENTARY USER ENTITY CONTROLS

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.

SUBSERVICE ORGANIZATIONS CARVED-OUT CONTROLS: MICROSOFT AZURE

The subservice organizations are expected to:

- Implement controls to enable security and monitoring tools within the production environment.

- Implement logical access security measures to infrastructure components including native security or security software and appropriate configuration settings.
- Restrict access to the virtual and physical servers, software, firewalls, and physical storage to authorized individuals and review the list of users and permissions on a regular basis.
- Implement controls to:
    - Provision access only to authorized persons.
    - Remove access when no longer appropriate.
    - Secure the facilities to permit access only to authorized persons.
    - Monitor access to the facilities.
- Be consistent with defined system security related to the design, acquisition, implementation, configuration modification, and management of infrastructure and software.
- Maintain system components, including configurations consistent with the defined system security, and related policies.
- Provide that only authorized tested and documented changes are made to the system.

SECTION IV: DESCRIPTION OF CRITERIA, CONTROLS, TESTS, & RESULTS OF TESTS

IV. DESCRIPTION OF CRITERIA, CONTROLS, TESTS, AND RESULTS OF TESTS

TESTING PERFORMED AND RESULTS OF TESTS OF ENTITY LEVEL CONTROLS

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of Keytos LLC and the tests performed by Decrypt Compliance and results are the responsibility of the service auditor.

RESULTS SUMMARY

DEVIATIONS NOTED	NO DEVIATIONS NOTED
2	80

NUMBER OF CONTROLS	82

CONTROL CRITERIA AND RELATED CONTROLS FOR SYSTEMS AND APPLICATIONS

On the pages that follow, the applicable control criteria and the controls to achieve the criteria have been specified by, and are the responsibility of, Keytos LLC. The sections “Tests Performed by Decrypt Compliance” and “Test Results” are the responsibility of Decrypt Compliance PC.

For tests of controls requiring the use of Information Produced by the Entity (IPE) (e.g., controls requiring system-generated populations for sample-based testing), Decrypt Compliance performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

(1) inspected the source of the IPE,
(2) inspected the query, script, or parameters used to generate the IPE,
(3) tied data between the IPE and the source, and/or
(4) inspected the IPE for anomalous gaps in sequence or timing to determine the data was complete, accurate, and maintained its integrity.

Furthermore, in addition to the above procedures, for tests of controls requiring management’s use of IPE in the execution of the controls (e.g., periodic reviews of user access listings); we inspect management’s procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

KEYTOS CONTROLS AND RELATED TRUST SERVICES CRITERIA

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	RELATED SOC 2 CRITERIA
DCF-1	Keytos Management has approved policies that detail how customer data may be made accessible and should be handled. These policies are accessible to employees and contractors.	CC2.1,CC5.2
DCF-2	Keytos authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	CC2.1,CC5.2
DCF-4	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.	CC6.7
DCF-5	Keytos's application code changes are reviewed by someone other than the person who made the code change prior to production deployment.	CC6.1,CC7.1,CC8.1
DCF-6	Only authorized Keytos personnel can push or make changes to production code.	CC7.1,CC8.1
DCF-7	Separate environments are used for testing and production for Keytos's application.	CC8.1
DCF-8	Keytos provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	CC8.1
DCF-9	Keytos provides a process to employees for reporting security incidents, and concerns, and other complaints to company management.	CC2.3
DCF-10	Access to systems at Keytos is granted only upon completion and approval of access request forms for new hires and employee transfers.	CC2.2,CC5.3
DCF-11	Keytos performs annual access control reviews.	CC4.1,CC6.2,CC6.3
DCF-12	Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Changes to the baseline configuration standards are monitored to log and flag any anomalies.	CC4.1,CC6.2,CC6.3,CC6.4
DCF-13	Keytos has a defined Information Security Policy that covers policies and procedures to	CC6.1

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	RELATED SOC 2 CRITERIA
	support the functioning of internal control.	
DCF-14	Keytos reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	CC2.1,CC5.3
DCF-15	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.	CC1.3,CC3.4,CC5.1
DCF-16	Keytos conducts a Risk Assessment at least annually.	CC3.1,CC3.2,CC5.1,CC5.3
DCF-17	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	CC1.2,CC2.1,CC3.1,CC3.2,CC3.3,CC3.4,CC4.1,CC4.2,CC5.1,CC5.2
DCF-19	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.	CC3.2,CC3.3,CC4.2,CC5.1,CC5.2
DCF-20	Keytos identifies, inventories, classifies, and assigns owners to IT assets.	CC1.2,CC3.1,CC3.4,CC4.1,CC4.2,CC5.1,CC5.2,CC7.1
DCF-21	Keytos maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control.	CC2.1,CC6.1
DCF-22	Keytos maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.	CC2.1
DCF-23	Keytos tracks and prioritizes security vulnerabilities weekly through internal tools according to severity. Critical/high vulnerabilities are remediated according to the vulnerability management policy.	CC6.1,CC6.6

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	RELATED SOC 2 CRITERIA
DCF-25	Keytos has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	CC7.2,CC7.3,CC7.4,CC7.5
DCF-26	Keytos conducts annual disaster recovery (DR) tests in alignment with its Disaster Recovery Plan. Test results are documented and reviewed to ensure recovery objectives are met and to support ongoing improvements to the plan.	CC5.3,CC9.1
DCF-27	Keytos utilizes multiple availability zones to replicate production data across different zones.	CC5.3
DCF-28	Keytos has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lending support to Business Continuity/Disaster Recovery.	CC9.1
DCF-29	Keytos has identified an incident response team that quantifies and monitors incidents involving security.	CC2.2,CC2.3,CC4.2,CC7.3,CC7.4,CC7.5,CC9.1
DCF-30	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.	CC2.2,CC2.3,CC4.2,CC7.3,CC7.4,CC7.5,CC9.1
DCF-31	Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	CC2.2,CC2.3,CC4.2,CC7.3,CC7.4,CC7.5,CC9.1
DCF-33	Management reviews security policies on an annual basis.	CC8.1
DCF-34	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.	CC1.2,CC5.3
DCF-36	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. Full-time employees are required to complete the training upon hire and annually thereafter.	CC1.2,CC1.3,CC4.2,CC5.1,CC5.2

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	RELATED SOC 2 CRITERIA
DCF-37	Keytos has established acceptable use of information assets approved by management. Personnel must acknowledge the Acceptable Use Policy upon hire.	CC1.4,CC1.5,CC2.2,CC5.2
DCF-38	Keytos evaluates the performance of employees through a formal, annual performance evaluation.	CC1.1,CC1.5,CC2.2
DCF-39	Keytos's new hires are required to pass a background check as a condition of their employment.	CC1.4,CC1.5
DCF-41	Members of the Board of Directors are independent of management.	CC1.1,CC1.4
DCF-42	Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	CC1.2
DCF-43	Keytos maintains a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and organization assets (physical or electronic) are properly returned.	CC1.2
DCF-44	Keytos has a formal Code of Conduct approved by management and accessible to employees. Personnel (including contractors) must acknowledge the Code of Conduct upon hire.	CC6.2,CC6.3,CC6.4,CC6.5
DCF-45	Keytos has established a Data Protection Policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy.	CC1.1,CC1.4,CC1.5,CC2.2,CC5.3
DCF-46	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.	CC1.1,CC2.2
DCF-47	Keytos positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Keytos.	CC1.4
DCF-48	Keytos ensures company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.	CC1.4
DCF-49	Keytos ensure employees use a password manager to save, store, and organize	CC6.6

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	RELATED SOC 2 CRITERIA
	passwords and logins in a personal vault protected on their devices.	
DCF-50	Keytos requires antivirus software to be installed on workstations to protect the network against malware.	CC6.1
DCF-51	Keytos ensures Operating System security patches are applied automatically on employees devices to reduce exposure to known vulnerabilities.	CC6.8
DCF-52	Keytos ensures that company-issued laptops have encrypted hard-disks.	CC6.8
DCF-53	Keytos has an established policy and procedures that governs the use of cryptographic controls.	CC6.1,CC6.7
DCF-54	Data at rest is encrypted using Transparent Data Encryption to ensure database files, transaction logs, and backups are encrypted using a database encryption key managed by a service-managed key.	CC2.1,CC5.2
DCF-55	Encryption on data in transit is enabled using a valid, authenticated HTTPS TLS 1.2 certificate, at minimum, to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	CC6.1,CC6.7
DCF-56	Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	CC6.6,CC6.7
DCF-57	Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	CC2.3,CC3.2,CC 3.4,CC4.1,CC4.2, CC6.4,CC9.2
DCF-58	Multi Factor Authentication is required to access Keytos cloud environment.	CC2.3,CC3.2,CC 6.4,CC9.2
DCF-59	Role-based security is in place for internal users including super admin users.	CC6.1,CC6.6
DCF-60	Keytos's application user passwords are stored using a salted password hash.	CC6.1,CC6.3
DCF-61	Keytos's customer data is segregated from the data of other customers.	CC6.1

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	RELATED SOC 2 CRITERIA
DCF-63	External users are required to review and accept the Terms of Service prior to account creation, ensuring access is granted only to verified individuals who acknowledge and agree to the organization's usage and security requirements.	CC6.7
DCF-64	Keytos's security commitments are communicated to external users, as appropriate.	CC6.6
DCF-65	Keytos maintains a Privacy Policy that is available to external users and internal employees, and it details the company's confidentiality and privacy commitments.	CC6.2,CC6.3
DCF-66	Keytos maintains a Terms of Service that is available to external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Client Agreements are in place for when the Terms of Service may not apply.	CC2.3
DCF-68	Keytos has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Strong password configuration settings, where applicable, are enabled, including: (1) Use a minimum of 8 characters (2) Use upper case, lower case, numeric, and special character values (3) Reuse prevention is limited to 24 versions (4) Multi factor authentication Phishing-resistant is enabled.	CC2.3
DCF-74	Keytos communicates system changes to customers that may affect security.	CC2.3
DCF-75	Cloud resources are configured to deny public access.	CC6.1,CC6.6
DCF-77	Keytos performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	CC6.6,CC6.7
DCF-80	Production systems and resources are monitored and automated alerts are sent out to personnel based on pre-configured rules.	CC2.3
DCF-85	Network security controls are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	CC6.6

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	RELATED SOC 2 CRITERIA
DCF-87	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.	CC7.5,CC9.1
DCF-88	A web application firewall is in place to protect public-facing web applications from outside threats.	CC7.2
DCF-90	Access to the root account in the cloud infrastructure provider is monitored. Login activity for the root account is investigated and validated for appropriateness.	CC6.6
DCF-91	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected. Critical/high incidents are resolved timely.	CC7.2
DCF-93	Keytos has an established key management process in place to support the organization's use of cryptographic techniques.	CC6.8,CC7.1,CC7.2
DCF-94	Keytos has documented requirements to ensure information assets are protected by physical controls that prevent tampering, damage, theft or unauthorized physical access.	CC6.6
DCF-109	Keytos has implemented a procedure to dispose of hardware containing sensitive data.	CC7.2
DCF-144	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	CC6.6,CC7.1,CC7.2
DCF-145	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls.	CC6.1
DCF-146	The Board of Directors meets annually, demonstrates independence from management, and exercises oversight of the development and performance of internal control.	CC6.4
DCF-150	Keytos uses DLP (Data Loss Prevention) software to prevent unencrypted sensitive information from being transmitted over email.	CC6.5
DCF-153	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	CC1.2

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	RELATED SOC 2 CRITERIA
	relevant findings.	
DCF-154	Keytos ensures that incident response plan testing is performed on an annual basis.	CC1.2
DCF-155	Keytos ensures that code changes are tested prior to deployment to ensure quality and security.	CC1.2
DCF-156	Keytos ensures that releases are approved by appropriate members of management prior to production release.	CC6.7
DCF-157	Keytos maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	CC2.1
DCF-159	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.	CC7.5

DESCRIPTION OF TEST OF CONTROLS AND RESULTS

SECURITY CATEGORY

Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
CC1.1 The entity demonstrates a commitment to integrity and ethical values.			
DCF-38	Keytos evaluates the performance of employees through a formal, annual performance evaluation.	Inquired of management to determine Keytos evaluates the performance of employees through a formal, annual performance evaluation. Inspected annual performance reviews to determine Keytos evaluates the performance of employees through a formal, annual performance evaluation.	No deviations noted.
DCF-41	Members of the Board of Directors are independent of management.	Inquired of management to determine members of the board of directors are independent of management. Inspected board meeting attendees to determine members of the board of directors are independent of management.	No deviations noted.
DCF-45	Keytos has established a Data Protection Policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy.	Inquired of management to determine that Keytos has established a data protection policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy. Inspected Data Protection Policy to determine that Keytos has established a data protection policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy. Inspected the policy acknowledgement overview and determined employees read and accepted the Data Protection Policy.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-46	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.	Inquired of management to determine 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. Inspected the recruitment records to determine Keytos's new hires and/or internal transfers completed screening to ensure that they are competent and capable of fulfilling their responsibilities.	No deviations noted.
CC1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
DCF-17	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inquired of management to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities. Inspected Risk Assessment Policy to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No deviations noted.
DCF-20	Keytos identifies, inventories, classifies, and assigns owners to IT assets.	Inquired of management to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets. Inspected the information asset inventory to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-34	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.	Inquired of management to determine 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 organizational chart and IS policy to determine 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.	No deviations noted.
DCF-36	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. Full-time employees are required to complete the training upon hire and annually thereafter.	Inquired of management to determine 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. Full-time employees are required to complete the training upon hire and annually thereafter. Inspected security awareness training completion records to determine employees completed security training timely.	No deviation noted. ***Deviation noted.*** *Personnel did not complete the annual security awareness training timely.*
DCF-42	Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	Inquired of management to determine that 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 management has established defined roles and responsibilities to oversee	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
		implementation of the information security policy across the organization.	
DCF-43	Keytos maintains a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and organization assets (physical or electronic) are properly returned.	Inquired of management to determine Keytos maintains a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and organization assets are properly returned. Inspected the termination checklist to determine Keytos maintains a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets are properly returned. Inspected a sample of terminated users to determine access for terminated users was removed in a timely manner.	No deviations noted.
DCF-153	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.	Inquired of management to determine 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 Internal audit report to determine Keytos performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Inspected the Internal audit report findings to determine no findings were detected that required corrective action to be taken.	No deviations noted.
DCF-154	Keytos ensures that incident response plan testing is performed on an annual basis.	Inquired of management to determine Keytos ensures that incident response plan testing is performed on an annual basis. Inspected the annual incident response plan testing results to determine it was performed timely.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-155	Keytos ensures that code changes are tested prior to deployment to ensure quality and security.	Inquired of management to determine Keytos ensures that code changes are tested prior to deployment to ensure quality and security. Inspected branch protection rules to determine Keytos ensures that code changes are tested prior to deployment to ensure quality and security.	No deviations noted.
CC1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
DCF-15	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.	Inquired of management to determine 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 Management policy to determine 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.	No deviations noted.
DCF-36	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. Full-time employees are required to complete the training upon hire and annually thereafter.	Inquired of management to determine 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. Full-time employees are required to complete the training upon hire and annually thereafter. Inspected security awareness training completion records to determine employees completed security training timely.	No deviation noted. ***Deviation noted.*** *Personnel did not complete the annual security*

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
			awareness training timely.
CC1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
DCF-37	Keytos has established acceptable use of information assets approved by management. Personnel must acknowledge the Acceptable Use Policy upon hire.	Inquired of management to determine Keytos has established acceptable use of information assets approved by management. Employees must acknowledge the Acceptable Use Policy upon hire. Inspected the Acceptable Use policy to determine Keytos has established acceptable use of information assets approved by management. Employees must acknowledge the acceptable use policy upon hire.	No deviations noted.
DCF-39	Keytos's new hires are required to pass a background check as a condition of their employment.	Inquired of management to determine Keytos's new hires are required to pass a background check as a condition of their employment. Inspected the onboarding process to determine Keytos's new hires are required to pass a background check as a condition of their employment. Inspected a sample of new hires to determine background checks were conducted as a condition of their employment.	No deviations noted.
DCF-41	Members of the Board of Directors are independent of management.	Inquired of management to determine members of the board of directors are independent of management. Inspected board meeting attendees to determine members of the board of directors are independent of management.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-45	Keytos has established a Data Protection Policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy.	Inquired of management to determine that Keytos has established a data protection policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy. Inspected Data Protection Policy to determine that Keytos has established a data protection policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy. Inspected the policy acknowledgement overview and determined employees read and accepted the Data Protection Policy.	No deviations noted.
DCF-47	Keytos positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Keytos.	Inquired of management to determine Keytos positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Keytos. Inspected the careers page to determine Keytos positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Keytos.	
DCF-48	Keytos ensures company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.	Inquired of management to determine Keytos ensures that all company-issued computers use a screensaver lock with a timeout of no more than 15 minutes. Inspected device security settings to determine Keytos ensures company issued computers use a screensaver lock with a timeout of no more than 15 minutes.	
CC1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-37	Keytos has established acceptable use of information assets approved by management. Personnel must acknowledge the Acceptable Use Policy upon hire.	Inquired of management to determine Keytos has established acceptable use of information assets approved by management. Employees must acknowledge the Acceptable Use Policy upon hire. Inspected the Acceptable Use policy to determine Keytos has established acceptable use of information assets approved by management. Employees must acknowledge the acceptable use policy upon hire.	No deviations noted.
DCF-38	Keytos evaluates the performance of employees through a formal, annual performance evaluation.	Inquired of management to determine Keytos evaluates the performance of employees through a formal, annual performance evaluation. Inspected annual performance reviews to determine Keytos evaluates the performance of employees through a formal, annual performance evaluation.	No deviations noted.
DCF-39	Keytos's new hires are required to pass a background check as a condition of their employment.	Inquired of management to determine Keytos's new hires are required to pass a background check as a condition of their employment. Inspected the onboarding process to determine Keytos's new hires are required to pass a background check as a condition of their employment. Inspected a sample of new hires to determine background checks were conducted as a condition of their employment.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-45	Keytos has established a Data Protection Policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy.	Inquired of management to determine that Keytos has established a data protection policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy. Inspected Data Protection Policy to determine that Keytos has established a data protection policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy. Inspected the policy acknowledgement overview and determined employees read and accepted the Data Protection Policy.	No deviations noted.
CC2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
DCF-1	Keytos Management has approved policies that detail how customer data may be made accessible and should be handled. These policies are accessible to employees and contractors.	Inquired of management to determine Keytos management has approved policies that detail how customer data may be made accessible and should be handled. These policies are accessible to employees and contractors. Inspected policies to determine Keytos management have approved policies that detail how customer data may be made accessible and should be handled. These policies are accessible to employees and contractors.	No deviations noted.
DCF-2	Keytos authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	Inquired of management to determine 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 role based access control matrix to determine Keytos authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-14	Keytos reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Inquired of management to determine that Keytos reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis. Inspected the organizational chart to determine the annual review of organizational structure, reporting lines, authorities, and responsibilities was completed timely.	No deviations noted.
DCF-17	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inquired of management to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities. Inspected Risk Assessment Policy to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No deviations noted.
DCF-21	Keytos maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control.	Inquired of management to determine Keytos maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control. Inspected the network architecture diagram to determine Keytos maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control.	No deviations noted.
DCF-22	Keytos maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.	Inquired of management to determine Keytos maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis. Inspected the network diagram to determine Keytos maintains an accurate network diagram that is accessible to the engineering team and is reviewed by management on an annual basis.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-54	Data at rest is encrypted using Transparent Data Encryption to ensure database files, transaction logs, and backups are encrypted using a database encryption key managed by a service-managed key.	Inquired of management to determine data at rest is encrypted using Transparent Data Encryption to ensure database files, transaction logs, and backups are encrypted using a database encryption key managed by a service-managed key. Inspected database encryption configuration to determine data at rest is encrypted using Transparent Data Encryption to ensure database files, transaction logs, and backups are encrypted using a database encryption key managed by a service-managed key.	No deviations noted.
DCF-157	Keytos maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inquired of management to determine Keytos maintains cybersecurity insurance to mitigate the financial impact of business disruptions. Inspected the cyber security insurance certification to determine Keytos maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	No deviations noted.
CC2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
DCF-10	Access to systems at Keytos is granted only upon completion and approval of access request forms for new hires and employee transfers.	Inquired of management to determine access to systems at Keytos is granted only upon completion and approval of access request forms for new hires and employee transfers. Inspected the System Access Control policy to determine access to systems at Keytos is granted only upon completion and approval of access request forms for all new hires and employee transfers. Inspected Microsoft Privileged Identity Management (PIM) to determine access to systems at Keytos is granted only upon completion and approval of access request forms for new hires and employee transfers.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-29	Keytos has identified an incident response team that quantifies and monitors incidents involving security.	Inquired of management to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security. Inspected the Information Security Plan to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security.	No deviations noted.
DCF-30	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.	Inquired of management to determine 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 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.	No deviations noted.
DCF-31	Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inquired of management to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes. Inspected Software Development LifeCycle Policy to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-37	Keytos has established acceptable use of information assets approved by management. Personnel must acknowledge the Acceptable Use Policy upon hire.	Inquired of management to determine Keytos has established acceptable use of information assets approved by management. Employees must acknowledge the Acceptable Use Policy upon hire. Inspected the Acceptable Use policy to determine Keytos has established acceptable use of information assets approved by management. Employees must acknowledge the acceptable use policy upon hire.	No deviations noted.
DCF-38	Keytos evaluates the performance of employees through a formal, annual performance evaluation.	Inquired of management to determine Keytos evaluates the performance of employees through a formal, annual performance evaluation. Inspected annual performance reviews to determine Keytos evaluates the performance of employees through a formal, annual performance evaluation.	No deviations noted.
DCF-45	Keytos has established a Data Protection Policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy.	Inquired of management to determine that Keytos has established a data protection policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy. Inspected Data Protection Policy to determine that Keytos has established a data protection policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy. Inspected the policy acknowledgement overview and determined employees read and accepted the Data Protection Policy.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-46	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.	Inquired of management to determine 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. Inspected the recruitment records to determine Keytos's new hires and/or internal transfers completed screening to ensure that they are competent and capable of fulfilling their responsibilities.	No deviations noted.
CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.			
DCF-9	Keytos provides a process to employees for reporting security incidents, and concerns, and other complaints to company management.	Inquired of management to determine Keytos provides a process to employees for reporting security incidents, and concerns, and other complaints to company management. Inspected security communication channel to determine Keytos provides a process to employees for reporting security incidents and concerns, and other complaints to company management.	No deviations noted.
DCF-29	Keytos has identified an incident response team that quantifies and monitors incidents involving security.	Inquired of management to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security. Inspected the Information Security Plan to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-30	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.	Inquired of management to determine 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 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.	No deviations noted.
DCF-31	Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inquired of management to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes. Inspected Software Development LifeCycle Policy to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No deviations noted.
DCF-57	Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inquired of management to determine that Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually. Inspected vendor compliance report review to determine Keytos critical vendor compliance reports are reviewed annually.	No deviation noted. ***Deviation noted*** *Review for critical vendor compliance reports was not documented.*

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-58	Multi Factor Authentication is required to access Keytos cloud environment.	Inquired of management to determine Multi Factor Authentication is required to access Keytos production environment. Inspected MFA configurations to determine Multi Factor Authentication are required to access Keytos cloud environment.	No deviations noted.
DCF-66	Keytos maintains a Terms of Service that is available to external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Client Agreements are in place for when the Terms of Service may not apply.	Inquired of management to determine Keytos maintains terms of service that are available to external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Client agreements are in place for when the terms of service may not apply. Inspected the Terms Of Use page to determine Keytos maintains terms of service that are available to external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems.	No deviations noted.
DCF-68	Keytos has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Strong password configuration settings, where applicable, are enabled, including: (1) Use a minimum of 8 characters (2) Use upper case, lower case, numeric, and special character values (3) Reuse prevention is limited to 24 versions (4) Multi factor authentication Phishing-resistant is enabled	Inquired of management to determine Keytos has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Inspected the Password Policy to determine Keytos has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Inspected password configuration to determine strong password configuration settings, where applicable, are enabled, including: (1) Use a minimum of 8 characters (2) Use upper case, lower case, numeric, and special character values (3) Reuse prevention is limited to 24 versions (4) Multi factor authentication Phishing-resistant is enabled	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-74	Keytos communicates system changes to customers that may affect security.	Inquired of management to determine Keytos communicates system changes to customers that may affect security. Inspected newsletter communication to determine Keytos communicates system changes to customers that may affect security.	No deviations noted.
DCF-80	Production systems and resources are monitored and automated alerts are sent out to personnel based on pre-configured rules.	Inquired of management to determine production systems and resources are monitored and automated alerts are sent out to personnel based on pre-configured rules. Inspected alert rules to determine production systems and resources are monitored and automated alerts are sent out to personnel based on pre-configured rules.	No deviations noted.
CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
DCF-16	Keytos conducts a Risk Assessment at least annually.	Inquired of management to determine Keytos conducts a risk assessment at least annually. Inspected the annual risk assessment report to determine the annual risk assessment was conducted timely.	No deviations noted.
DCF-17	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inquired of management to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities. Inspected Risk Assessment Policy to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-20	Keytos identifies, inventories, classifies, and assigns owners to IT assets.	Inquired of management to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets. Inspected the information asset inventory to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets.	No deviations 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.			
DCF-16	Keytos conducts a Risk Assessment at least annually.	Inquired of management to determine Keytos conducts a risk assessment at least annually. Inspected the annual risk assessment report to determine the annual risk assessment was conducted timely.	No deviations noted.
DCF-17	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inquired of management to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities. Inspected Risk Assessment Policy to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No deviations noted.
DCF-19	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.	Inquired of management to determine 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 penetration test report to determine Keytos engages with third-party to conduct penetration tests of the production environment at least annually.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
		Inspected penetration test reports to determine Keytos results are reviewed by management and no high priority findings were detected.	
DCF-57	Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inquired of management to determine that Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually. Inspected vendor compliance report review to determine Keytos critical vendor compliance reports are reviewed annually.	No deviation noted. ***Deviation noted*** *Review for critical vendor compliance reports was not documented.*
DCF-58	Multi Factor Authentication is required to access Keytos cloud environment.	Inquired of management to determine Multi Factor Authentication is required to access Keytos production environment. Inspected MFA configurations to determine Multi Factor Authentication are required to access Keytos cloud environment.	No deviations noted.
CC3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
DCF-17	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inquired of management to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities. Inspected Risk Assessment Policy to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-19	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.	Inquired of management to determine 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 penetration test report to determine Keytos engages with third-party to conduct penetration tests of the production environment at least annually. Inspected penetration test reports to determine Keytos results were reviewed by management and no high priority findings were detected.	No deviations noted.
CC3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.			
DCF-15	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.	Inquired of management to determine 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 Management policy to determine 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.	No deviations noted.
DCF-17	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inquired of management to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities. Inspected Risk Assessment Policy to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-20	Keytos identifies, inventories, classifies, and assigns owners to IT assets.	Inquired of management to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets. Inspected the information asset inventory to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets.	No deviations noted.
DCF-57	Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inquired of management to determine that Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually. Inspected vendor compliance report review to determine Keytos critical vendor compliance reports are reviewed annually.	No deviation noted. ***Deviation noted*** *Review for critical vendor compliance reports was not documented.*
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.			
DCF-11	Keytos performs annual access control reviews.	Inquired of management to determine that Keytos performs annual access control reviews. Inspected access control review to determine that Keytos performs annual access control reviews.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-12	Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Changes to the baseline configuration standards are monitored to log and flag any anomalies.	Inquired of management to determine Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Changes to the baseline configuration standards are monitored to log and flag any anomalies. Inspected baseline configurations to determine Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Inspected monitoring schedule configuration to determine changes to the baseline configuration standards are monitored to log and flag any anomalies.	No deviations noted.
DCF-17	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inquired of management to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities. Inspected Risk Assessment Policy to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No deviations noted.
DCF-20	Keytos identifies, inventories, classifies, and assigns owners to IT assets.	Inquired of management to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets. Inspected the information asset inventory to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-57	Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inquired of management to determine that Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually. Inspected vendor compliance report review to determine Keytos critical vendor compliance reports are reviewed annually.	No deviation noted. ***Deviation noted*** *Review for critical vendor compliance reports was not documented.*
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.			
DCF-17	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inquired of management to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities. Inspected Risk Assessment Policy to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No deviations noted.
DCF-19	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.	Inquired of management to determine 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 penetration test report to determine Keytos engages with third-party to conduct penetration tests of the production environment at least annually.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
		Inspected penetration test reports to determine Keytos results were reviewed by management and no high priority findings were detected.	
DCF-20	Keytos identifies, inventories, classifies, and assigns owners to IT assets.	Inquired of management to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets. Inspected the information asset inventory to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets.	No deviations noted.
DCF-29	Keytos has identified an incident response team that quantifies and monitors incidents involving security.	Inquired of management to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security. Inspected the Information Security Plan to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security.	No deviations noted.
DCF-30	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.	Inquired of management to determine 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 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.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-31	Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inquired of management to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes. Inspected Software Development LifeCycle Policy to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No deviations noted.
DCF-36	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. Full-time employees are required to complete the training upon hire and annually thereafter.	Inquired of management to determine 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. Full-time employees are required to complete the training upon hire and annually thereafter. Inspected security awareness training completion records to determine employees completed security training timely.	No deviation noted. ***Deviation noted.*** *Personnel did not complete the annual security awareness training timely.*
DCF-57	Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inquired of management to determine that Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually. Inspected vendor compliance report review to determine Keytos critical vendor compliance reports are reviewed annually.	No deviation noted. ***Deviation noted*** *Review for critical vendor compliance*

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
			reports was not documented.
CC5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
DCF-15	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.	Inquired of management to determine 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 Management policy to determine 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.	No deviations noted.
DCF-16	Keytos conducts a Risk Assessment at least annually.	Inquired of management to determine Keytos conducts a risk assessment at least annually. Inspected the annual risk assessment report to determine the annual risk assessment was conducted timely.	No deviations noted.
DCF-17	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inquired of management to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities. Inspected Risk Assessment Policy to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-19	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.	Inquired of management to determine 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 penetration test report to determine Keytos engages with third-party to conduct penetration tests of the production environment at least annually. Inspected the penetration test report to determine Keytos results were reviewed by management and no high priority findings were detected.	No deviations noted.
DCF-20	Keytos identifies, inventories, classifies, and assigns owners to IT assets.	Inquired of management to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets. Inspected the information asset inventory to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets.	No deviations noted.
DCF-36	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. Full-time employees are required to complete the training upon hire and annually thereafter.	Inquired of management to determine 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. Full-time employees are required to complete the training upon hire and annually thereafter. Inspected security awareness training completion records to determine employees completed security training timely.	No deviation noted. ***Deviation noted.*** *Personnel did not complete the annual security awareness training timely.*

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
CC5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.			
DCF-1	Keytos Management has approved policies that detail how customer data may be made accessible and should be handled. These policies are accessible to employees and contractors.	Inquired of management to determine Keytos management has approved policies that detail how customer data may be made accessible and should be handled. These policies are accessible to employees and contractors. Inspected policies to determine Keytos management have approved policies that detail how customer data may be made accessible and should be handled. These policies are accessible to employees and contractors.	No deviations noted.
DCF-2	Keytos authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	Inquired of management to determine 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 role based access control matrix to determine Keytos authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.	No deviations noted.
DCF-17	Keytos's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inquired of management to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities. Inspected Risk Assessment Policy to determine Keytos's management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-19	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.	Inquired of management to determine 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 the penetration test report to determine Keytos engages with third-party to conduct penetration tests of the production environment at least annually. Inspected the penetration test report to determine Keytos results were reviewed by management and no high priority findings were detected.	No deviations noted.
DCF-20	Keytos identifies, inventories, classifies, and assigns owners to IT assets.	Inquired of management to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets. Inspected the information asset inventory to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets.	No deviations noted.
DCF-36	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. Full-time employees are required to complete the training upon hire and annually thereafter.	Inquired of management to determine 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. Full-time employees are required to complete the training upon hire and annually thereafter. Inspected security awareness training completion records to determine employees completed security training timely.	No deviation noted. ***Deviation noted.*** *Personnel did not complete the annual security awareness training timely.*

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-37	Keytos has established acceptable use of information assets approved by management. Personnel must acknowledge the Acceptable Use Policy upon hire.	Inquired of management to determine Keytos has established acceptable use of information assets approved by management. Employees must acknowledge the Acceptable Use Policy upon hire. Inspected the Acceptable Use policy to determine Keytos has established acceptable use of information assets approved by management. Employees must acknowledge the acceptable use policy upon hire.	No deviations noted.
DCF-54	Data at rest is encrypted using Transparent Data Encryption to ensure database files, transaction logs, and backups are encrypted using a database encryption key managed by a service-managed key.	Inquired of management to determine data at rest is encrypted using Transparent Data Encryption to ensure database files, transaction logs, and backups are encrypted using a database encryption key managed by a service-managed key. Inspected database encryption configuration to determine data at rest is encrypted using Transparent Data Encryption to ensure database files, transaction logs, and backups are encrypted using a database encryption key managed by a service-managed key.	No deviations noted.
CC5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
DCF-10	Access to systems at Keytos is granted only upon completion and approval of access request forms for new hires and employee transfers.	Inquired of management to determine access to systems at Keytos is granted only upon completion and approval of access request forms for new hires and employee transfers. Inspected the System Access Control policy to determine access to systems at Keytos is granted only upon completion and approval of access request forms for all new hires and employee transfers. Inspected Microsoft Privileged Identity Management (PIM) to determine access to systems at Keytos is granted only upon completion and approval of access request forms for new hires and employee transfers.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-14	Keytos reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	Inquired of management to determine that Keytos reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis. Inspected the organizational chart to determine the annual review of organizational structure, reporting lines, authorities, and responsibilities was completed timely.	No deviations noted.
DCF-16	Keytos conducts a Risk Assessment at least annually.	Inquired of management to determine Keytos conducts a risk assessment at least annually. Inspected the annual risk assessment report to determine the annual risk assessment was conducted timely.	No deviations noted.
DCF-26	Keytos conducts annual disaster recovery (DR) tests in alignment with its Disaster Recovery Plan. Test results are documented and reviewed to ensure recovery objectives are met and to support ongoing improvements to the plan.	Inquired of management to determine Keytos conducts annual disaster recovery (DR) tests in alignment with its Disaster Recovery Plan. Test results are documented and reviewed to ensure recovery objectives are met and to support ongoing improvements to the plan. Inspected the DR test report to determine Keytos conducts annual disaster recovery (DR) tests in alignment with its Disaster Recovery Plan. Test results are documented and reviewed to ensure recovery objectives are met and to support ongoing improvements to the plan.	No deviations noted.
DCF-27	Keytos utilizes multiple availability zones to replicate production data across different zones.	Inquired of management to determine Keytos utilizes multiple availability zones to replicate production data across different zones. Inspected Azure available regions to determine Keytos utilizes multiple availability zones to replicate production data across different zones.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-34	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.	Inquired of management to determine 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 organizational chart and IS policy to determine 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.	No deviations noted.
DCF-45	Keytos has established a Data Protection Policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy.	Inquired of management to determine that Keytos has established a data protection policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy. Inspected Data Protection Policy to determine that Keytos has established a data protection policy and requires employees to acknowledge it upon hire. Management monitors employees' acceptance of the policy. Inspected the policy acknowledgement overview and determined employees read and accepted the Data Protection Policy.	No deviations 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.			
DCF-5	Keytos's application code changes are reviewed by someone other than the person who made the code change prior to production deployment.	Inquired of management to determine Keytos's application code changes are reviewed by someone other than the person who made the code change prior to production deployment. Inspected the source code tool configuration to determine code review is required prior to deploying the changes to the production environment.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-13	Keytos has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inquired of management to determine 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 Keytos has a defined information security policy that covers policies and procedures to support the functioning of internal control.	No deviations noted.
DCF-21	Keytos maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control.	Inquired of management to determine Keytos maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control. Inspected the network architecture diagram to determine Keytos maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control.	No deviations noted.
DCF-23	Keytos tracks and prioritizes security vulnerabilities weekly through internal tools according to severity. Critical/high vulnerabilities are remediated according to the vulnerability management policy.	Inquired of management to determine Keytos tracks and prioritizes security vulnerabilities through internal tools according to severity. Critical/high vulnerabilities are remediated according to the vulnerability management policy. Inspected the Vulnerability Management Policy to determine vulnerability handling timelines are defined to ensure vulnerabilities are resolved timely according to severity. Inspected the production vulnerability scanner to determine Keytos tracks and prioritizes security vulnerabilities through internal tools according to severity. Inspected vulnerability scan results to determine critical/high vulnerabilities are remediated timely.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-50	Keytos requires antivirus software to be installed on workstations to protect the network against malware.	Inquired of management to determine Keytos requires antivirus software to be installed on workstations to protect the network against malware. Inspected device security settings to determine antivirus software is installed on workstations.	No deviations noted.
DCF-53	Keytos has an established policy and procedures that governs the use of cryptographic controls.	Inquired of management to determine that Keytos has an established policy and procedures that governs the use of cryptographic controls. Inspected the Encryption policy to determine that Keytos has an established policy and procedures that governs the use of cryptographic controls.	No deviations noted.
DCF-55	Encryption on data in transit is enabled using a valid, authenticated HTTPS TLS 1.2 certificate, at minimum, to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	Inquired of management to determine encryption on data in transit is enabled using a valid, authenticated HTTPS TLS 1.2 certificate, at minimum, to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet. Inspected company's web application domain configuration to determine encryption on data in transit is enabled using a valid, authenticated HTTPS TLS 1.2 certificate, at minimum.	No deviations noted.
DCF-59	Role-based security is in place for internal users including super admin users.	Inquired of management to determine that role-based security is in place for internal users, including super admin users. Inspected Azure IAM role assignments to determine role-based security is in place for internal including super admin users.	No deviations noted.
DCF-60	Keytos's application user passwords are stored using a salted password hash.	Inquired of management to determine Keytos's application user passwords are stored using a salted password hash.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
		Inspected the password manager to determine Keytos's application user passwords are stored using a salted password hash.	
DCF-61	Keytos's customer data is segregated from the data of other customers.	Inquired of management to determine Keytos's customer data is segregated from the data of other customers. Inspected the customers' database to determine Keytos's customer data is segregated from the data of other customers.	No deviations noted.
DCF-75	Cloud resources are configured to deny public access.	Inquired of management to determine cloud resources are configured to deny public access. Inspected networking SQL server access configuration to determine cloud resources are configured to deny public access.	No deviations noted.
DCF-145	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls.	Inquired of management to determine the company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. Inspected Board of Directors profiles to determine the company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls.	No deviations 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.			
DCF-11	Keytos performs annual access control reviews.	Inquired of management to determine that Keytos performs annual access control reviews. Inspected access control review to determine that Keytos performs annual access control reviews.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-12	Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Changes to the baseline configuration standards are monitored to log and flag any anomalies.	Inquired of management to determine Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Changes to the baseline configuration standards are monitored to log and flag any anomalies. Inspected baseline configurations to determine Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Inspected monitoring schedule configuration to determine changes to the baseline configuration standards are monitored to log and flag any anomalies.	No deviations noted.
DCF-44	Keytos has a formal Code of Conduct approved by management and accessible to employees. Personnel (including contractors) must acknowledge the Code of Conduct upon hire.	Inquired of management to determine Keytos has a formal code of conduct approved by management and accessible to personnel. Personnel (including contractors) must acknowledge the code of conduct upon hire. Inspected Code of Conduct document to determine Keytos has a formal code of conduct approved by management. Personnel (including contractors) must acknowledge the code of conduct upon hire.	No deviations noted.
DCF-65	Keytos maintains a Privacy Policy that is available to external users and internal employees, and it details the company's confidentiality and privacy commitments.	Inquired of management to determine Keytos maintains a privacy policy that is available to external users and internal employees and it details the company's confidentiality and privacy commitments. Inspected the Privacy Policy to determine Keytos maintains a privacy policy that is available to external users and internal employees, and it details the company's confidentiality and privacy commitments.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
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.			
DCF-11	Keytos performs annual access control reviews.	Inquired of management to determine that Keytos performs annual access control reviews. Inspected access control review to determine that Keytos performs annual access control reviews.	No deviations noted.
DCF-12	Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Changes to the baseline configuration standards are monitored to log and flag any anomalies.	Inquired of management to determine Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Changes to the baseline configuration standards are monitored to log and flag any anomalies. Inspected baseline configurations to determine Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Inspected monitoring schedule configuration to determine changes to the baseline configuration standards are monitored to log and flag any anomalies.	No deviations noted.
DCF-44	Keytos has a formal Code of Conduct approved by management and accessible to employees. Personnel (including contractors) must acknowledge the Code of Conduct upon hire.	Inquired of management to determine Keytos has a formal code of conduct approved by management and accessible to personnel. Personnel (including contractors) must acknowledge the code of conduct upon hire. Inspected Code of Conduct document to determine Keytos has a formal code of conduct approved by management. Personnel (including contractors) must acknowledge the code of conduct upon hire.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-60	Keytos's application user passwords are stored using a salted password hash.	Inquired of management to determine Keytos's application user passwords are stored using a salted password hash. Inspected the password manager to determine Keytos's application user passwords are stored using a salted password hash.	No deviations noted.
DCF-65	Keytos maintains a Privacy Policy that is available to external users and internal employees, and it details the company's confidentiality and privacy commitments.	Inquired of management to determine Keytos maintains a privacy policy that is available to external users and internal employees and it details the company's confidentiality and privacy commitments. Inspected the Privacy Policy to determine Keytos maintains a privacy policy that is available to external users and internal employees, and it details the company's confidentiality and privacy commitments.	No deviations 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.			
DCF-12	Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Changes to the baseline configuration standards are monitored to log and flag any anomalies.	Inquired of management to determine Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Changes to the baseline configuration standards are monitored to log and flag any anomalies. Inspected baseline configurations to determine Keytos maintains a baseline security configuration standards for system components, aligning with industry best practices or vendor guidance. Inspected monitoring schedule configuration to determine changes to the baseline configuration standards are monitored to log and flag any anomalies.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-44	Keytos has a formal Code of Conduct approved by management and accessible to employees. Personnel (including contractors) must acknowledge the Code of Conduct upon hire.	Inquired of management to determine Keytos has a formal code of conduct approved by management and accessible to personnel. Personnel (including contractors) must acknowledge the code of conduct upon hire. Inspected Code of Conduct document to determine Keytos has a formal code of conduct approved by management. Personnel (including contractors) must acknowledge the code of conduct upon hire.	No deviations noted.
DCF-57	Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inquired of management to determine that Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually. Inspected vendor compliance report review to determine Keytos critical vendor compliance reports are reviewed annually.	No deviation noted. ***Deviation noted*** *Review for critical vendor compliance reports was not documented.*
DCF-58	Multi Factor Authentication is required to access Keytos cloud environment.	Inquired of management to determine Multi Factor Authentication is required to access Keytos production environment. Inspected MFA configurations to determine Multi Factor Authentication are required to access Keytos cloud environment.	No deviations noted.
DCF-146	The Board of Directors meets annually, demonstrates independence from management, and exercises oversight of the development and performance of internal control.	Inquired of management to determine that the Board of Directors meets annually, demonstrates independence from management, and exercises oversight of the development and performance of internal control.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
		Inspected annual board meeting minutes to determine the company's board of directors meets at least annually, demonstrates independence from management, and exercises oversight of the development and performance of internal control.	
Microsoft Azure is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.			
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.			
DCF-44	Keytos has a formal Code of Conduct approved by management and accessible to employees. Personnel (including contractors) must acknowledge the Code of Conduct upon hire.	Inquired of management to determine Keytos has a formal code of conduct approved by management and accessible to personnel. Personnel (including contractors) must acknowledge the code of conduct upon hire. Inspected Code of Conduct document to determine Keytos has a formal code of conduct approved by management. Personnel (including contractors) must acknowledge the code of conduct upon hire.	No deviations noted.
DCF-150	Keytos uses DLP (Data Loss Prevention) software to prevent unencrypted sensitive information from being transmitted over email	Inquired of management to determine that Keytos uses DLP (data loss prevention) software to prevent unencrypted sensitive information from being transmitted over email. Inspected Microsoft Purview platform to determine Keytos uses data loss prevention (DLP) software to prevent unencrypted sensitive information from being transmitted over email.	No deviations noted.
Microsoft Azure is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting where the services reside. Microsoft Azure is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.			

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
DCF-23	Keytos tracks and prioritizes security vulnerabilities weekly through internal tools according to severity. Critical/high vulnerabilities are remediated according to the vulnerability management policy.	Inquired of management to determine Keytos tracks and prioritizes security vulnerabilities through internal tools according to severity. Critical/high vulnerabilities are remediated according to the vulnerability management policy. Inspected the Vulnerability Management Policy to determine vulnerability handling timelines are defined to ensure vulnerabilities are resolved timely according to severity. Inspected the production vulnerability scanner to determine Keytos tracks and prioritizes security vulnerabilities through internal tools according to severity. Inspected vulnerability scan results to determine critical/high vulnerabilities are remediated timely.	No deviations noted.
DCF-49	Keytos ensure employees use a password manager to save, store, and organize passwords and logins in a personal vault protected on their devices.	Inquired of management to determine Keytos ensure employees use a password manager to save, store, and organize passwords and logins in a personal vault protected on their devices. Inspected employees' devices to determine a password manager are installed to save, store, and organize passwords and logins in a personal vault protected on their devices.	No deviations noted.
DCF-56	Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inquired of management to determine Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities. Inspected the vendor information inventory to determine Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-59	Role-based security is in place for internal users including super admin users.	Inquired of management to determine that role-based security is in place for internal users, including super admin users. Inspected Azure IAM role assignments to determine role-based security is in place for internal including super admin users.	No deviations noted.
DCF-64	Keytos's security commitments are communicated to external users, as appropriate.	Inquired of management to determine Keytos's security commitments are communicated to external users, as appropriate. Inspected the Master Service agreement to determine Keytos's security commitments are communicated to external users, as appropriate. Inspected a vendor contractor to determine Keytos's security commitments are communicated as appropriate.	No deviations noted.
DCF-75	Cloud resources are configured to deny public access.	Inquired of management to determine cloud resources are configured to deny public access. Inspected networking SQL server access configuration to determine cloud resources are configured to deny public access.	No deviations noted.
DCF-77	Keytos performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	Inquired of management to determine that Keytos performs backups daily and retains them in accordance with a predefined schedule in the backup policy. Inspected the Backup policy to determine management has a predefined schedule for backups to ensure Inspected backup configurations to determine Keytos performs backups daily and retains them in accordance with a predefined schedule in the backup policy.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-85	Network security controls are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	Inquired of management to determine that network security controls are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied. Inspected network security configurations to determine network security controls are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.	No deviations noted.
DCF-90	Access to the root account in the cloud infrastructure provider is monitored. Login activity for the root account is investigated and validated for appropriateness.	Inquired of management to determine access to the root account in the cloud infrastructure provider is monitored. login activity for the root account is investigated and validated for appropriateness. Inspected Azure Monitor alert rules to determine access to the root account in the cloud infrastructure provider is monitored.	No deviations noted.
DCF-94	Keytos has documented requirements to ensure information assets are protected by physical controls that prevent tampering, damage, theft or unauthorized physical access.	Inquired of management to determine Keytos has documented requirements to ensure information assets are protected by physical controls that prevent tampering, damage, theft or unauthorized physical access. Inspected the Physical Security policy to determine Keytos has documented requirements to ensure information assets are protected by physical controls that prevent tampering, damage, theft or unauthorized physical access.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-144	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inquired of management to determine that the company's board of directors has a documented charter that outlines its oversight responsibilities for internal control. Inspected Board of Directors Charter to determine that the company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	No deviations 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.			
DCF-4	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.	Inquired of management to determine 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. Inspected version control configuration to determine Keytos uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Inspected source control tool access to determine access to the source code tool is approved by a system admin.	No deviations noted.
DCF-53	Keytos has an established policy and procedures that governs the use of cryptographic controls.	Inquired of management to determine that Keytos has an established policy and procedures that governs the use of cryptographic controls. Inspected the Encryption policy to determine that Keytos has an established policy and procedures that governs the use of cryptographic controls.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-55	Encryption on data in transit is enabled using a valid, authenticated HTTPS TLS 1.2 certificate, at minimum, to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	Inquired of management to determine encryption on data in transit is enabled using a valid, authenticated HTTPS TLS 1.2 certificate, at minimum, to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet. Inspected company's web application domain configuration to determine encryption on data in transit is enabled using a valid, authenticated HTTPS TLS 1.2 certificate, at minimum.	No deviations noted.
DCF-56	Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inquired of management to determine Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities. Inspected the vendor information inventory to determine Keytos maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	No deviations noted.
DCF-63	External users are required to review and accept the Terms of Service prior to account creation, ensuring access is granted only to verified individuals who acknowledge and agree to the organization's usage and security requirements.	Inquired of management to determine external users are required to review and accept the Terms of Service prior to account creation, ensuring access is granted only to verified individuals who acknowledge and agree to the organization's usage and security requirements. Inspected the subscription page to determine external users are required to review and accept the Terms of Service prior to account creation.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-77	Keytos performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	Inquired of management to determine that Keytos performs backups daily and retains them in accordance with a predefined schedule in the backup policy. Inspected the Backup policy to determine management has a predefined schedule for backups to ensure Inspected backup configurations to determine Keytos performs backups daily and retains them in accordance with a predefined schedule in the backup policy.	No deviations noted.
DCF-156	Keytos ensures that releases are approved by appropriate members of management prior to production release.	Inquired of management to determine Keytos ensures that releases are approved by appropriate members of management prior to production release. Inspected Github protection rules to determine Keytos ensures that releases are approved by appropriate members of management prior to production release.	No deviations 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.			
DCF-51	Keytos ensures Operating System security patches are applied automatically on employees devices to reduce exposure to known vulnerabilities.	Inquired of management to determine Keytos ensures Operating System security patches are applied automatically on employees devices to reduce exposure to known vulnerabilities. Inspected device security settings to determine Keytos ensures Operating System security patches are applied automatically on employees devices to reduce exposure to known vulnerabilities.	No deviations noted.
DCF-52	Keytos ensures that company-issued laptops have encrypted hard-disks.	Inquired of management to determine Keytos ensures that company-issued laptops have encrypted hard-disks.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
		Inspected device security settings to determine Keytos ensures that company-issued laptops have encrypted hard-disks.	
DCF-93	Keytos has an established key management process in place to support the organization's use of cryptographic techniques.	Inquired of management to determine the company has an established key management process in place to support the organization's use of cryptographic techniques. Inspected the Encryption Management policy to determine the company has an established key management process to support the organization's use of cryptographic techniques Inspected the company's Microsoft Azure Key Management System (KMS) module to determine for Microsoft Azure-managed keys, the company uses 256-bit encryption algorithms and implements annual key rotation via Microsoft Azure KMS module.	No deviations 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.			
DCF-5	Keytos's application code changes are reviewed by someone other than the person who made the code change prior to production deployment.	Inquired of management to determine Keytos's application code changes are reviewed by someone other than the person who made the code change prior to production deployment. Inspected the source code tool configuration to determine code review is required prior to deploying the changes to the production environment.	No deviations noted.
DCF-6	Only authorized Keytos personnel can push or make changes to production code.	Inquired of management to determine that only authorized Keytos personnel can push or make changes to production code. Inspected GitHub branch protection rules to determine only authorized Keytos personnel can push or make changes to production code.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-20	Keytos identifies, inventories, classifies, and assigns owners to IT assets.	Inquired of management to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets. Inspected the information asset inventory to determine that Keytos identifies, inventories, classifies, and assigns owners to IT assets.	No deviations noted.
DCF-93	Keytos has an established key management process in place to support the organization's use of cryptographic techniques.	Inquired of management to determine the company has an established key management process in place to support the organization's use of cryptographic techniques. Inspected the Encryption Management policy to determine the company has an established key management process to support the organization's use of cryptographic techniques Inspected the company's Microsoft Azure Key Management System (KMS) module to determine for Microsoft Azure-managed keys, the company uses 256-bit encryption algorithms and implements annual key rotation via Microsoft Azure KMS module.	No deviations noted.
DCF-144	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inquired of management to determine that the company's board of directors has a documented charter that outlines its oversight responsibilities for internal control. Inspected Board of Directors Charter to determine that the company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	No deviations 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.			

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-25	Keytos has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inquired of management to determine 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 Keytos has an established disaster recovery plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	No deviations noted.
DCF-88	A web application firewall is in place to protect public-facing web applications from outside threats.	Inquired of management to determine a web application firewall is in place to protect public-facing web applications from outside threats. Inspected the Microsoft Azure Front Door interface to determine a web application firewall is in place to protect public-facing web applications from outside threats.	No deviations noted.
DCF-91	An intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected. Critical/high incidents are resolved timely.	Inquired of management to determine that an intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected. Inspected the intrusion detection system to determine an intrusion detection system (IDS) is in place to detect potential intrusions, alert personnel when a potential intrusion is detected. Inspected security alerts to determine no critical/high issues were detected during the attest period.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-93	Keytos has an established key management process in place to support the organization's use of cryptographic techniques.	Inquired of management to determine the company has an established key management process in place to support the organization's use of cryptographic techniques. Inspected the Encryption Management policy to determine the company has an established key management process to support the organization's use of cryptographic techniques Inspected the company's Microsoft Azure Key Management System (KMS) module to determine for Microsoft Azure-managed keys, the company uses 256-bit encryption algorithms and implements annual key rotation via Microsoft Azure KMS module.	No deviations noted.
DCF-109	Keytos has implemented a procedure to dispose of hardware containing sensitive data.	Inquired of management to determine Keytos has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data. Inspected relevant policy and procedure documents to determine Keytos has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	No deviations noted.
DCF-144	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inquired of management to determine that the company's board of directors has a documented charter that outlines its oversight responsibilities for internal control. Inspected Board of Directors Charter to determine that the company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	No deviations 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.			

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-25	Keytos has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inquired of management to determine 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 Keytos has an established disaster recovery plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	No deviations noted.
DCF-29	Keytos has identified an incident response team that quantifies and monitors incidents involving security.	Inquired of management to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security. Inspected the Information Security Plan to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security.	No deviations noted.
DCF-30	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.	Inquired of management to determine 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 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.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-31	Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inquired of management to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes. Inspected Software Development LifeCycle Policy to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No deviations 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.			
DCF-25	Keytos has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inquired of management to determine 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 Keytos has an established disaster recovery plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	No deviations noted.
DCF-29	Keytos has identified an incident response team that quantifies and monitors incidents involving security.	Inquired of management to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security. Inspected the Information Security Plan to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-30	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.	Inquired of management to determine 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 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.	No deviations noted.
DCF-31	Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inquired of management to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes. Inspected Software Development LifeCycle Policy to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No deviations noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
DCF-25	Keytos has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inquired of management to determine 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 Keytos has an established disaster recovery plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-29	Keytos has identified an incident response team that quantifies and monitors incidents involving security.	Inquired of management to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security. Inspected the Information Security Plan to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security.	No deviations noted.
DCF-30	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.	Inquired of management to determine 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 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.	No deviations noted.
DCF-31	Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inquired of management to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes. Inspected Software Development LifeCycle Policy to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-87	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.	Inquired of management to determine 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 logging and monitoring policy to determine 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 Microsoft Defender for Cloud security alerts to determine Keytos has infrastructure logging configured to monitor web traffic and suspicious activity and alerts are investigated and remediated.	No deviations noted.
DCF-159	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.	Inquired of management to determine 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 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.	No deviations 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.			

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-5	Keytos's application code changes are reviewed by someone other than the person who made the code change prior to production deployment.	Inquired of management to determine Keytos's application code changes are reviewed by someone other than the person who made the code change prior to production deployment. Inspected the source code tool configuration to determine code review is required prior to deploying the changes to the production environment.	No deviations noted.
DCF-6	Only authorized Keytos personnel can push or make changes to production code.	Inquired of management to determine that only authorized Keytos personnel can push or make changes to production code. Inspected GitHub branch protection rules to determine only authorized Keytos personnel can push or make changes to production code.	No deviations noted.
DCF-7	Separate environments are used for testing and production for Keytos's application.	Inquired of management to determine separate environments are used for testing and production for Keytos's application. Inspected the Keytos application environments portals to determine that separate environments are used for testing and production environments of Keytos's application.	No deviations noted.
DCF-8	Keytos provides a process to external users for reporting security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints.	Inquired of management to determine Keytos provides a process to external users for reporting security failures, incidents concerns and other complaints. Inspected the company's application and website to determine Keytos provides a process to external users for reporting security failures, incidents concerns and other complaints.	No deviations noted.
DCF-33	Management reviews security policies on an annual basis.	Inquired of management to determine management reviews security policies on an annual basis.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
		Inspected the security policies to determine annual management reviews were conducted timely.	
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
DCF-26	Keytos conducts annual disaster recovery (DR) tests in alignment with its Disaster Recovery Plan. Test results are documented and reviewed to ensure recovery objectives are met and to support ongoing improvements to the plan.	Inquired of management to determine Keytos conducts annual disaster recovery (DR) tests in alignment with its Disaster Recovery Plan. Test results are documented and reviewed to ensure recovery objectives are met and to support ongoing improvements to the plan. Inspected the DR test report to determine Keytos conducts annual disaster recovery (DR) tests in alignment with its Disaster Recovery Plan. Test results are documented and reviewed to ensure recovery objectives are met and to support ongoing improvements to the plan.	No deviations noted.
DCF-28	Keytos has implemented an Incident Response Plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lending support to Business Continuity/Disaster Recovery.	Inquired of management to determine Keytos has implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lending support to business continuity/disaster recovery. Inspected the Incident Response plan to determine Keytos has implemented an incident response plan that includes creating, prioritizing, assigning, and tracking follow-ups to completion and lending support to business continuity/disaster recovery.	No deviations noted.
DCF-29	Keytos has identified an incident response team that quantifies and monitors incidents involving security.	Inquired of management to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security. Inspected the Information Security Plan to determine Keytos has identified an incident response team that quantifies and monitors incidents involving security.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-30	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.	Inquired of management to determine 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 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.	No deviations noted.
DCF-31	Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inquired of management to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes. Inspected Software Development LifeCycle Policy to determine Keytos has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
DCF-87	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.	Inquired of management to determine 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 logging and monitoring policy to determine 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 Microsoft Defender for Cloud security alerts to determine Keytos has infrastructure logging configured to monitor web traffic and suspicious activity and alerts are investigated and remediated.	No deviations noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
DCF-57	Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inquired of management to determine that Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually. Inspected vendor compliance report review to determine Keytos critical vendor compliance reports are reviewed annually.	No deviation noted. ***Deviation noted*** *Review for critical vendor compliance reports was not documented.*
DCF-58	Multi Factor Authentication is required to access Keytos cloud environment.	Inquired of management to determine Multi Factor Authentication is required to access Keytos production environment.	No deviations noted.

CONTROL #	CONTROLS SPECIFIED BY KEYTOS	TESTS PERFORMED BY DECRYPT COMPLIANCE & TEST RESULTS	
		Inspected MFA configurations to determine Multi Factor Authentication are required to access Keytos cloud environment.	

SECTION V:
OTHER INFORMATION PROVIDED BY KEYTOS

V. OTHER INFORMATION PROVIDED BY KEYTOS

Management Response to the Deviation Identified

Deviation #1

Related Criteria: CC1.2, CC1.3, CC4.2, CC5.1, CC5.2

Control DCF-36: 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. Full-time employees are required to complete the training upon hire and annually thereafter.

Deviation: Three personnel did not complete the annual security awareness training timely.

Compensating Controls: DCF-1, DCF-2, DCF-15, DCF-16, DCF-17, DCF-19, DCF-20, DCF-29, DCF-30, DCF-31, ,DCF-34, DCF-36, DCF-37, DCF-42, DCF-43, DCF-54, DCF-57, DCF-153, DCF-154, DCF-155

Management Response:

An error was identified in our training tracking platform that caused the training status to incorrectly display as completed (green), even though some users had not yet taken the training for the year. This issue was promptly corrected by our provider. As soon as the discrepancy was discovered, all affected users completed the 2025 security awareness training.

Additionally, we are confident in our staff's ongoing security knowledge. Every Monday, management conducts a weekly security learning session where we discuss recent industry security incidents, review how we protect our infrastructure, and cover relevant security topics.

Improvements Implemented After the Attestation Period:
Following the attestation period, we worked with Drata to ensure the root cause of the tracking error was fully resolved. We also verified that all employees completed the 2025 training.

Commitment to Continuous Improvement:
We are committed to implementing additional safeguards to detect and prevent similar issues in the future, ensuring our security program remains robust and compliant.

Deviation #2:

Related Criteria: CC2.3, CC3.2, CC3.4, CC4.1, CC4.2, CC6.4, CC9.2

DCF-57: Keytos maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.

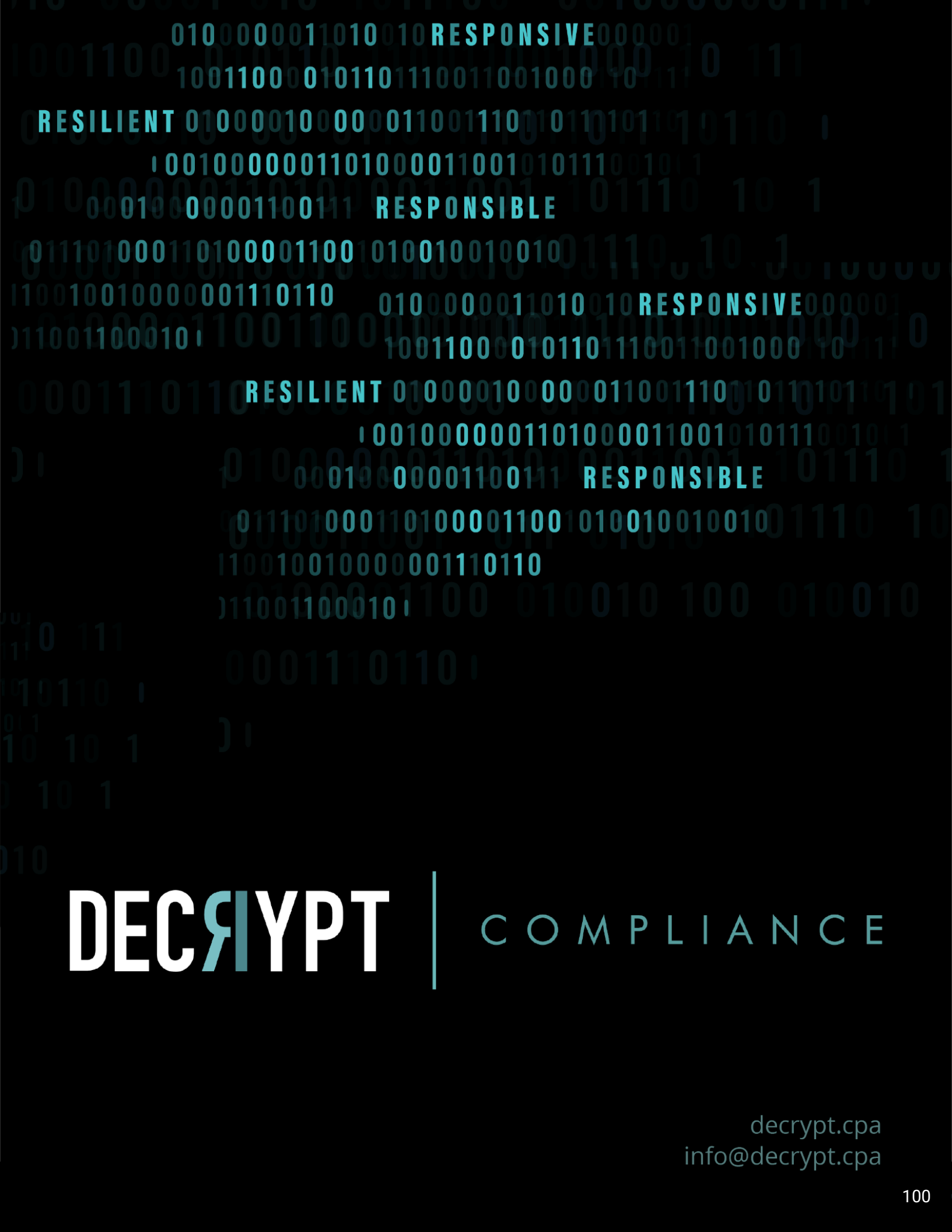
Deviation: Review for critical vendor compliance reports was not documented.

Compensating Controls: DCF-9, DCF-11, DCF-12, DCF-15, DCF-16, DCF-17, DCF-19, DCF-20, DCF-29, DCF-30, DCF-31, DCF-36, DCF-44, DCF-56, DCF-57, DCF-58, DCF-66, DCF-68, DCF-74, DCF-80, DCF-146

Management response:
Management did review the SOC 2 reports for key vendors during the attestation period. However, since no concerns were identified, the review was not formally documented. We acknowledge this oversight and understand the importance of maintaining clear evidence of such reviews, regardless of findings.

Improvements Implemented After the Attestation Period
Management has updated the review process to ensure that all vendor compliance report evaluations are documented, including instances where no issues are identified.

Commitment to Continuous Improvement
We are committed to enhancing our documentation practices and internal controls to ensure full transparency and compliance with our vendor management procedures.



DECRYPT | COMPLIANCE

decrypt.cpa
info@decrypt.cpa

Title	Please sign Keytos Final SOC2 Type II Report
File name	Copy_of_Keytos_SO...Draft_Report_.pdf
Document ID	1ffd71abaae9cfbf2820a60674d6ce4cd0050095
Audit trail date format	MM / DD / YYYY
Status	Signed

Document history

E-SIGN DISCLOSURE ACCEPTED	**01 / 29 / 2024** 22:54:48 UTC	Electronic record and signature disclosure accepted by Raymond Cheng (rcheng@decrypt.cpa) IP: 185.211.32.97 GUID: 64c4266d5570849b04ce8a19d1cfe026eef30842
SENT	**07 / 03 / 2025** 17:01:45 UTC	Sent for signature to Raymond Cheng (rcheng@decrypt.cpa) from rcheng@decrypt.cpa IP: 41.150.224.218
VIEWED	**07 / 03 / 2025** 18:08:14 UTC	Viewed by Raymond Cheng (rcheng@decrypt.cpa) IP: 73.189.177.180
SIGNED	**07 / 03 / 2025** 18:08:26 UTC	Signed by Raymond Cheng (rcheng@decrypt.cpa) IP: 73.189.177.180
COMPLETED	**07 / 03 / 2025** 18:08:26 UTC	The document has been completed.