Tokeny Solutions

SOC 2 Type 1 Report

For the

T-REX Platform

An Independent Service Auditor’s Report on the Suitability of the Design of Controls Relevant to Security

July 31, 2023

Assurance | Tax | Advisory | Wealth Management
Minneapolis • Naples

TABLE OF CONTENTS

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

BOULAY

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Tokeny Solutions:

Scope

We have examined Tokeny Solution's ('Tokeny' or the 'service organization') accompanying description of its digital asset management system found in Section III, titled "Description of the T-REX Platform" as of July 31, 2023 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design of controls stated in the description as of July 31, 2023, to provide reasonable assurance that Tokeny's service commitments and system requirements would be achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

Tokeny uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud computing and data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Tokeny, to achieve Tokeny's service commitments and system requirements based on the applicable trust services criteria. The description presents Tokeny's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Tokeny's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

The information included in Section V, "Other Information Provided by Tokeny" is presented by Tokeny's management to provide additional information and is not part of Tokeny's description of its digital asset management system made available to user entities as of July 31, 2023. Information about management's response to the testing exception has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

Service Organization's Responsibilities

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

Service Auditor’s Responsibilities

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

An examination of a description of a service organization’s system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and the service organization’s service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is 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
- Evaluating the overall presentation of the description

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their information needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Basis for Qualified Opinion

The accompanying description of the digital asset management system states on page 15 that risk management is primarily the responsibility of the security team, which performs periodic risk assessments that identify and document the significant risks facing the organization, including any fraud risks. The results of these risk assessments determine the development and implementation of controls, operating procedures, and compliance processes for addressing and mitigating such risks.

However, testing procedures performed in Section IV, “Trust Services Categories, Criteria, and Related Controls Relevant to Security” noted that Tokeny did not maintain insurance to mitigate the financial impact of business disruptions, including cyber incidents.

As a result, controls were not suitably designed as of July 31, 2023, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the trust services criterion:

- *CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.*

Opinion

In our opinion, in all material respects,

a. the description presents Tokeny's digital asset management system that was designed and implemented as of July 31, 2023 in accordance with the description criteria.

b. except for the effects of the matter giving rise to the modification described in the *Basis for Qualified Opinion* section above, the controls stated in the description were suitably designed as of July 31, 2023 to provide reasonable assurance that Tokeny's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Tokeny's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Tokeny, user entities of Tokeny's system as of July 31, 2023, business partners of Tokeny subject to risks arising from interactions with Tokeny's system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the services provided by the service organization
- How the service organization's system interacts with user entities, business partners, the subservice organization, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- 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.

Boulay PLLP

Minneapolis, Minnesota
August 23, 2023

SECTION II

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Tokeny Solution's (Tokeny) digital asset management system titled "Description of the T-REX Platform" as of July 31, 2023 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about the digital asset management system that may be useful when assessing the risks arising from interactions with Tokeny's system, particularly information about system controls that Tokeny has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

Tokeny uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud computing and data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Tokeny, to achieve Tokeny's service commitments and system requirements based on the applicable trust services criteria. The description presents Tokeny's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Tokeny's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Tokeny, to achieve Tokeny's service commitments and system requirements based on the applicable trust services criteria. The description presents Tokeny's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Tokeny's controls.

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

a. the description presents Tokeny's digital asset management system that was designed and implemented as of July 31, 2023 in accordance with the description criteria.

b. except for the effects of the matter described in paragraph c, the controls stated in the description were suitably designed as of July 31, 2023 to provide reasonable assurance that Tokeny's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Tokeny's controls as of that date.

c. testing procedures performed in Section IV, "Trust Services Categories, Criteria, and Related Controls Relevant to Security" noted that Tokeny did not maintain insurance to mitigate the financial impact of business disruptions, including cyber incidents.

Luc Falempin

Luc Falempin
Chief Executive Officer
Tokeny

SECTION III

DESCRIPTION OF THE T-REX PLATFORM

DESCRIPTION OF THE T-REX PLATFORM

Company Background

Founded in 2017, Tokeny (‘Tokeny’ or ‘the Company’) is a technology company that provides an enterprise-grade infrastructure to allow companies and financial actors to compliantly issue, transfer, and manage assets on blockchain networks, enabling them to improve operational efficiency and asset liquidity. Tokeny is headquartered in Luxembourg and has over 30 professionals globally. More information can be found on the Company’s website at tokeny.com.

Description of Services Provided

The T-REX platform is a scalable and secure solution that allows asset owners and their authorized agents to digitally and compliantly issue, allocate and manage tokenized securities, whilst providing an improved user experience and highly transferable securities for their investors.

The provided compliance framework is asset and jurisdictionally agnostic thanks to the built-in onchain identity system. The T-REX platform is available in SaaS by APIs and/or white-label GUI.

Below is a quick summary of the components of the platform and Tokeny’s associated solutions:

- Servicing – Management platform for token holders and token actions:
    - Deploy ERC3643 tokens easily with the built-in token factory
    - Manage token information (supply, price, category, logo, documents, etc.)
    - Automated registry of token holders with positions, names, etc. to track ownership of assets
    - Generate Position reports at any date to perform corporate actions
    - Mint, Burn, Pause, Block, Unblock, Force transfer. One by one or by batch transactions
    - Manage admin users and smart contracts Agents
    - Wallet connection via connected or integrated wallet solutions
    - Gas tank feature available for integrated wallets (users don’t need to buy utility tokens and manage gas fees when they perform transactions)
    - By default, the Servicing is T-REX branded. It can be white labeled by simple request

Features of the platform for **investors** include:

- Qualification – White-label solution to onboard and qualify token holders:
    - Create a digital onboarding funnel for investors
    - Manage pipeline and track investors
    - Authorized/banned countries
    - Workflows management by investor type (corporate, individuals)
    - Information request (exhaustive list of fields and custom fields)
    - Collection of documents
    - Integration with automated KYC solutions for ID verifications, “Liveness”, Video interview, Sanction lists
    - Onchain whitelisting: deploying digital identities and whitelisting eligible token holders’ identities
    - White labeling: URL, colors, images, transactional emails, token documents, and information
    - Applicants management on the Servicing

- Subscription – White-label solution to allow token subscription and payments:
    - Choose payment methods (fiats, stablecoins, and/or cryptocurrencies)
    - Automatic issuer fees for intended subscription
    - Sign subscription documents electronically (DocuSign integration)
    - Reconcile payments and manage exchange rates
    - Mint tokens to investors’ wallets
    - Orders management on the Servicing

- Investor Portal – Offer a digital and functional management interface to investors:
    - Digital securities management portal for investors
    - See holdings and transactions
    - Perform transfers (direct transfers, conditional transfers, Delivery versus Delivery (DvD) transfers)
    - Receive messages and news from the issuer
    - Identity and profile management
    - White labeling: URL, colors, images, transactional emails, token documents, and information
    - Gas tank feature available for integrated wallets
- Marketplace – Multi-token white-label front-end interfaces for marketplace operators and their investors:
    - White labeling: URL, colors, images, transactional emails, token documents, and information
    - See the listing of offerings
    - See the details of offerings
    - See portfolios
    - Secondary market Billboard multi-token
    - Identity and profile management
- Billboard – Improve the liquidity for your investors whilst relying on encoded T-REX compliance. License-exempted P2P secondary market solution:
    - Allow investors to discover one another through bulletin boards
    - Enable investors to publish buy and sell offers to facilitate transfers
    - Compatible with DINO and DvD/atomic swap transfers
- DINO – Distribution network for security tokens. Publish tokens to the network of Marketplaces to maximize your audience of investors:
    - Primary market projects made available on the network
    - Secondary market offers made available on the network

Principal Service Commitments and System Requirements

Tokeny designs its processes and procedures to meet its objectives for its services. Those objectives are based on the service commitments that Tokeny makes to user entities and regulations that govern the provisioning of services, and the financial, operational and compliance requirements that Tokeny has established for the services. Security commitments to user entities are documented and communicated in the Terms of Service and Terms of Use, as well as in the description of the service offerings provided online. Security commitments are standardized and include, but are not limited to, the following:

- Implementing security measures that comply with the highest standards in force, under an obligation of means against unauthorized access or damage to data,
- Using the best in security practices to ensure the safety of its data and code best-in-class security practices to ensure the safety of its data and code, and
- Using reasonable efforts to secure and fix any breach as soon as possible.

Tokeny establishes operational requirements that support the achievement of security commitments, relevant regulations, and other system requirements. Such requirements are communicated in Tokeny’s policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around system design, development, and operations, as well as management of internal business systems and networks. 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 Tokeny’s system.

Components of the System

Infrastructure

Tokeny operates a cloud-based network within Amazon Web Services (AWS), which provides secure hosting of network and production systems. The key infrastructure components are noted in the table below.

Component	Purpose
VPC (Virtual Private Cloud)	virtual network used to isolate and secure Tokeny's environments
ALB (Application Load Balancer)	entry point of all external communications which aims to secure the traffic (SSL encryption), load balance the load/requests and protects against potential cyber attack
ECS (Elastic Container Service)	AWS fully managed container orchestration service used to run Tokeny's applications services
RDS (Relational Database Service)	AWS fully managed relational database service used to run Tokeny's databases (PostgreSQL and MySQL), this service also handle backups/snapshots
DynamoDB	AWS fully managed NoSQL database used for specific Tokeny's services (needed for performance and scalability)
Lambda	AWS serverless computing service used to run scheduled/event-based services

Software

Primary software used to support the digital asset management system include the following:

Software	Purpose
T-REX Servicing Investor	Portal for investors to manage their security tokens, initiate transfers and subscribe to token offerings
T-REX Servicing Issuer	Admin portal for token issuers / operators to manage investors, KYC, subscription, redemption, token supply
Qualification Platform	Digital onboarding and automatic KYC process (3rd party processed data)
T-REX Factory	Admin portal for token issuers / operators to deploy T-REX to the blockchain
Marketplace	Investor portal for primary market investments

People

Tokeny maintains a staff of over 30 professionals across the functional areas of executive management, technology, commercial, marketing and operations.

Executive Management

The executive management team incorporates the following individuals:

- Chief Executive Officer (CEO)
- Chief Technology Officer (CTO)
- Chief Commercial Officer (CCO)
- Chief Operations Officer (COO)
- Head of Product

Technology

The CTO oversees the technology group, which incorporates product development, innovation and engineering.

Commercial, Marketing & Operations

The CEO oversees marketing, legal, human resources and administration. The CCO oversees the commercial development of the Company.

Data

Tokeny classifies data based on the degree of confidentiality required using the following labels:

- **Confidential**: This information is the most private or otherwise sensitive and must be monitored and controlled at all times.
- **Sensitive**: This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access.
- **Internal**: This information is intended for use only within Tokeny, and in some cases within affiliated organizations.

Any data file or printed document that is not labeled and contains sensitive data is considered classified as “Internal” and handled accordingly.

Procedures

The following security policies and procedures are maintained and updated at least annually by Tokeny:

- Access Control
- Asset Management
- Business Continuity and Disaster Recovery Plan
- Change Management
- Code of Ethics
- Cryptography
- Data Retention and Disposal
- Incident Response
- Information Security
- Key Management
- Personnel Security
- Risk Management
- Vendor Management

Tokeny employees and contractors are required to acknowledge their understanding of the policies and procedures upon hire.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

Control Environment

Management’s Philosophy

Integrity and ethical values are essential elements of management’s philosophy and Tokeny’s control environment. The executive leadership team are responsible for setting the example of ethical conduct at Tokeny and communicating expectations across the organization through the Code of Ethics policy.

Security Management

The CTO is the designation information security officer at Tokeny. The CTO is responsible for creating and enforcing security policies and procedures, leading the monitoring, vulnerability management, incident detection and response initiatives, and minimizing risk across the organization.

All Tokeny employees are required to attend information security awareness training on an annual basis to ensure that personnel are knowledgeable of risks and controls around cybersecurity and data protection.

Personnel Security

New positions that are posted at Tokeny have clearly defined job descriptions and outline the technical and educational requirements the Company is seeking in prospective candidates. Background checks are performed on new employees and contractors prior to their start date. Once employed, personnel are subject to Tokeny's procedures around information security. A provisioning ticket is submitted to the IT team requesting that the newly hired employee or contractor obtain the system access necessary to perform their job. Access is granted based on the principle of least privilege.

Physical Security and Environmental Controls

The in-scope systems and infrastructure that support Tokeny are hosted by AWS (see *Complementary Subservice Organization Controls* section below). The Company's Asset Management Policy outlines requirements around securing physical laptops and include disciplinary actions for those who violate the policy.

Logical Security

Tokeny uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Employees sign on to the Tokeny production network using their Google Workspace (GSuite) credentials, which includes two-factor authentication. Users are also required to separately sign on to any systems or applications that do not use Google SSO functionality.

Customers access the T-REX platform through the Internet using HTTPS. In all cases, connections that encrypt passwords before they will fully function. Users must supply a valid user ID, password and MFA.

Change Management

Tokeny maintains documented Change Management policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and user acceptance testing results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

The GitHub version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. GitHub maintains a history of code changes to support rollback capabilities and tracks changes to developers.

System Monitoring

Tokeny management performs system monitoring activities to continuously assess the quality of internal control over time and ensure that any corrective actions are completed in a timely manner. Examples of system monitoring processes in place include:

- Firewalls – Systems that filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized.
- Vulnerability Scanning – Continuous process by which infrastructure and software is automatically tested for security weaknesses.
- Penetration Testing – Web application penetration testing to identify, and subsequently remediate, vulnerabilities that can be exploited by bad actors.

Problem Management

Security incidents and other IT-related issues are reported to the incident management team. Issues are tracked using the Company's ticketing system and are monitored to ensure timely resolution.

Risk Assessment Process

Tokeny conducts an enterprise-wide risk assessment at least annually using the OneTrust security compliance platform. This application enables Tokeny to categorize risks to the business, describe their cause and potential impact, and outline mitigation steps to reduce the likelihood and impact.

Risk management is primarily the responsibility of the security team, which performs periodic risk assessments that identify and document the significant risks facing the organization, including any fraud risks. The results of these risk assessments determine the development and implementation of controls, operating procedures, and compliance processes for addressing and mitigating such risks. Tokeny policies require that any instances of suspected or actual fraud be brought to the immediate attention of senior management, the security team, or human resources.

Information and Communication Systems

Tokeny employees and contractors are able to access all information security policies within the OneTrust security compliance platform and these policies are acknowledged upon hire. Additionally, Tokeny uses email and Slack as communication tools across the organization. As all personnel work remotely, frequent team meetings are held virtually.

Monitoring Controls

Monitoring controls are built into Tokeny's management responsibilities. On a weekly basis, management meets to discuss issues impacting Tokeny. Topics for discussion include financial performance, strategic planning, human resources, and information security. Any strategic initiatives or process changes that are decided upon in these meetings are communicated to appropriate personnel in each department.

As the CTO is part of Tokeny's security team, any important topics related to information security would be communicated in timely manner to the rest of management, either through the weekly management meetings, via Slack, or other communication methods based on the level of severity.

Ongoing Monitoring

Tokeny's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective actions through management meetings, Slack communication channels, and informal notifications.

Management's close involvement in Tokeny's operations helps to identify significant variances from expectations regarding internal controls. Management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the Company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Tokeny personnel.

Reporting Deficiencies

Tokeny utilizes Jira as a ticketing system to document and track reported system incidents to resolution. Reported issues are prioritized based on severity ratings and a formal incident response plan is triggered if necessary.

Control Objectives and Related Controls

Tokeny's control objectives and description of related controls are included in Section IV, "Trust Services Categories, Criteria and Related Controls Relevant to Security." Although the control objectives and related controls are included in Section IV, they are an integral part of the description of the digital asset management system.

Complementary User Entity Controls (CUECs)

Tokeny's controls cover only a portion of overall internal control for each user entity of the digital asset management system. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by Tokeny. Therefore, each user entity's internal controls should be evaluated in conjunction with Tokeny's controls, considering the related CUECs identified for the specific criterion. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal controls to determine whether the identified CUECs have been implemented and are operating effectively.

The user entity controls presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Control Activity
CC6.1	• User entities maintain logical access security to the T-REX Platform by ensuring unique user IDs, complex passwords and two-factor authentication. • User entities are responsible for the hardware, software, network connections and technical safeguards needed for its use of the Tokeny services.
CC6.2 CC6.3	• User entities restrict access to the T-REX Platform based on the principle of least privilege.
CC7.4 CC7.5	• User entities notify Tokeny immediately of any unauthorized use of user content, account or any other breach of security.

Complementary Subservice Organization Controls (CSOCs)

Tokeny’s primary hosting is with AWS, a subsidiary of Amazon that provides on-demand cloud computing platforms to individuals, companies, and governments, on a paid subscription basis. The technology allows subscribers to have at their disposal a virtual cluster of computers, available all the time, through the Internet.

Tokeny’s services are designed with the assumption that certain controls will be implemented at AWS. Such controls are called complementary subservice organization controls. It is not feasible for the service commitments, system requirements, and applicable criteria related to the digital asset management system to be achieved solely by Tokeny. Therefore, each user entity’s internal controls must be evaluated in conjunction with Tokeny’s controls, considering the related CSOCs expected to be implemented at the subservice organization, as described below.

Criteria	Control Activity
CC6.4	• AWS is responsible for restricting data center access to authorized personnel. • AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC9.1	• AWS is responsible for the installation of fire suppression, detection, and environmental monitoring systems at the data centers. • AWS is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterrupted power supply. • AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

Tokeny receives and reviews the AWS SOC 2 Type 2 report annually. In addition, through its operational activities, Tokeny monitors the services performed by AWS to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Tokeny also has communication with the subservice organization to monitor compliance with the service agreement, stay up to date on planned changes at the hosting facility, and communicate any issues or concerns to AWS management.

System Incidents

There were no identified system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure to the achievement of one or more of those service commitments and system requirements as of July 31, 2023.

Trust Services Criteria Not Applicable

All criteria within the security category was applicable to the digital asset management system.

Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how the system is used to provide services as of July 31, 2023.

SECTION IV

TRUST SERVICES CATEGORIES, CRITERIA, AND RELATED CONTROLS RELEVANT TO SECURITY

SECURITY

Control #	Control Activity Specified by Tokeny
Control Environment	
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	
CC1.1.1	Tokeny has established a Corporate Ethics policy that is acknowledged by all new employees and contractors upon hire. This policy outlines expectations the Company has set related to ethics and standards of conduct. Additionally, this policy outlines processes that management has established to evaluate adherence to standards of conduct and address deviations in a timely manner.
CC1.1.2	Tokeny maintains a whistleblower hotline that enables the anonymous reporting of ethical concerns to executive leadership.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
CC1.2.1	Tokeny has a Board of Directors that is made up of independent leaders with relevant skills and industry expertise, which enables them to provide credible challenge and oversight over management.
CC1.2.2	The Board of Directors meet with management on a quarterly basis to discuss Company performance, strategic objectives and information security matters.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
CC1.3.1	Tokeny maintains an organizational chart that establishes structure, reporting lines, and delegation of authority and responsibility across the Company.
CC1.3.2	Tokeny has an assigned security team that is responsible for the design, implementation, and oversight of the organization’s security policies and procedures. The security team communicates important information security events to management in a timely manner.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
CC1.4.1	All positions have a detailed job description that lists qualifications, such as required skills and experience, which candidates must meet in order to be hired by Tokeny.
CC1.4.2	Background checks are performed on new hires before the new hire's start date, as permitted by local laws. The results are reviewed by HR and appropriate action is taken if deemed necessary.
CC1.4.3	On a quarterly basis, management and the Board of Directors review the competency of its staff against the required business objectives and forecasted growth to determine whether additional resources are necessary.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
CC1.5.1	Tokeny maintains formalized performance expectations for each position and uses these expectations as a basis for evaluating the performance of each of its employees. These performance evaluations, which incorporate internal control responsibilities, are completed on an annual basis.

Control #	Control Activity Specified by Tokeny
Communication and Information	
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	
CC2.1.1	Tokeny's mission-critical systems and sensitive information are identified during the annual risk assessment, which includes capturing internal and external sources of data.
CC2.1.2	Tokeny maintains a network diagram outlining how data is processed and secured.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
CC2.2.1	Tokeny maintains updated policies and procedures that enable all personnel to understand and carry out their internal control responsibilities. These policies and procedures are accessible to all personnel and are acknowledged upon hire.
CC2.2.2	Tokeny employees are required to complete an annual Information Security Awareness training.
CC2.2.3	Tokeny provides a process for employees and contractors to report security incidents, concerns, and other complaints to management.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	
CC2.3.1	Tokeny maintains an updated Privacy Policy on its website that communicates the Company's commitment to privacy to external users. The policy provides a contact method for questions or complaints.
CC2.3.2	Tokeny enables inbound communications from customers and other stakeholders by maintaining contact information on their website for general inquiries, customer support, partnerships, and public relations.
CC2.3.3	Objective descriptions of Tokeny's system and its boundaries are available to authorized external users and customers.

Control #	Control Activity Specified by Tokeny
Risk Assessment	
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
CC3.1.1	Tokeny maintains an updated Risk Assessment Program that describes the processes the Company has in place to identify new business and technical risks and how those risks are mitigated.
CC3.1.2	At least annually, Tokeny conducts an assessment on the risks related to information security, physical security, vendor management and fraud.
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
CC3.2.1	At least annually, Tokeny performs a risk assessment, which includes the identification of relevant internal and external threats, an analysis of the significance of the risks associated with those threats, a determination of appropriate risk mitigation strategies, and the development or modification of controls consistent with the risk mitigation strategy.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	
CC3.3.1	As part of the risk assessment process, management conducts a fraud assessment that considers various types of fraud exposure and identifies controls that mitigate the risk of fraud.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	
CC3.4.1	As part of the risk assessment process, management identifies and assesses changes that could significantly impact the system of internal control. The assessment includes evaluating changes relates to information security, physical security, vendor management and fraud.

Control #	Control Activity Specified by Tokeny
Monitoring Activities	
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
CC4.1.1	Tokeny conducts ongoing monitoring over internal controls to ensure they are appropriately designed and operating effectively in accordance with baseline requirements. These evaluations are conducted by knowledgeable personnel, integrate with business processes, consider changes in business processes, and vary in frequency based on associated risks.
CC4.1.2	Tokeny engages a qualified third-party security firm to conduct a web application penetration test at least annually. Results are reviewed by management and high-priority findings are remediated in a timely manner.
CC4.1.3	Tokeny has implemented a vulnerability management program to detect and remediate system vulnerabilities in software packages used in the Company’s infrastructure.
CC4.1.4	Tokeny has established a formalized phishing prevention and monitoring campaign to evaluate employee and contractor response to potential social engineering attacks.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and board of directors, as appropriate.	
CC4.2.1	Management assesses the results of ongoing and separate evaluations. Deficiencies are communicated to relevant parties for corrective action and management tracks whether the deficiencies are remediated in a timely manner.

Control #	Control Activity Specified by Tokeny
Control Activities	
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
CC5.1.1	As part of the risk assessment process, management ensures that adequate controls are in place to mitigate the identified risks to an acceptable level. Considerations in the identification and implementation of control activities include entity-specific factors, relevant business processes, incorporating a mix of control activity types (manual, automated, preventive, detective) and segregation of duties.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	
CC5.2.1	Tokeny maintains a suite of Information Technology General Controls (ITGCs) to support the achievement of objectives. These ITGCs are identified as part of the annual risk assessment completed by management and cover areas such as technology infrastructure, security management as well as technology acquisition, development, and maintenance.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	
CC5.3.1	Tokeny maintains updated policies and procedures that incorporate control activities across the organization. These policies and procedures establish requirements pertaining to timely performance of controls, taking corrective action on control deficiencies, and ensuring that competent personnel are accountable for control execution.

Control #	Control Activity Specified by Tokeny
Logical and Physical Access Controls	
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.	
CC6.1.1	Tokeny maintains an updated inventory of information assets within the organization.
CC6.1.2	Access to Tokeny's systems and applications requires complex passwords and multi-factor authentication (MFA).
CC6.1.3	Tokeny utilizes password managers to store encrypted passwords in the cloud.
CC6.1.4	Tokeny utilizes Virtual Private Clouds (VPCs) and sub-networks (subnets) to achieve network segmentation in its AWS cloud-based environment.
CC6.1.5	Tokeny utilizes AWS's Identity and Access Management (IAM) to securely manage access to AWS services and resources. IAM enables the Company to create and manage AWS users/groups and use permissions to allow and deny access to AWS resources.
CC6.1.6	Tokeny maintains active SHA-256 encryption certificates for its web application to ensure secure connections for its users.
CC6.1.7	Tokeny encrypts data at-rest through server-side encryption (SSE) using AES-256.
CC6.1.8	Tokeny encrypts all employee and contractor workstations with full disk encryption.
CC6.1.9	Tokeny utilizes AWS Key Management Service to create and manage keys and control the use of encryption across its cloud-based environment.
CC6.1.10	Tokeny maintains a secure administrator account that manages the system. Administrative rights are granted only to individuals who require access to fulfill their job responsibilities.
Please reference *Complementary User Entity Controls (CUECs)* in Section III for additional controls that are to be implemented by user entities.	
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.	
CC6.2.1	The system administrator approves system access for newly hired personnel, as well as access change requests.
CC6.2.2	System access is removed within 24 hours upon employee or contractor termination.
CC6.2.3	On at least a quarterly basis, the CTO reviews access rights for all Tokeny employees to ensure that system access is appropriate. Any access rights that are no longer needed are removed following this review.
Please reference *Complementary User Entity Controls (CUECs)* in Section III for additional controls that are to be implemented by user entities.	

Control #	Control Activity Specified by Tokeny
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.	
CC6.3.1	The system administrator approves system access for newly hired personnel, as well as access change requests.
CC6.3.2	System access is removed within 24 hours upon employee or contractor termination.
CC6.3.3	On at least a quarterly basis, the CTO reviews access rights for all Tokeny employees to ensure that system access is appropriate. Any access rights that are no longer needed are removed following this review.
Please reference *Complementary User Entity Controls (CUECs)* in Section III for additional controls that are to be implemented by user entities.	
CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
Testing was not applicable for this criterion, as Tokeny did not have a physical office space as of July 31, 2023 (all employees worked remotely). Additionally, Tokeny uses AWS to provide cloud computing and data center hosting services. Please reference *Complementary Subservice Organization Controls (CSOCs*) in Section III for controls that are to be implemented by the subservice organization.	
CC6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read and recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.5.1	Tokeny has a Data Deletion Policy that outlines how data is deleted in connection with the cancellation or termination of an Tokeny account.
CC6.5.2	Prior to disposing of obsolete workstations or removable media, the CISO ensures that all physical devices are sanitized to remove any confidential information.
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.6.1	Firewall rules are configured to restrict network traffic to approved ports, protocols, and sources.
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.	
CC6.7.1	Tokeny utilizes a Virtual Private Network (VPN) to enable secure remote access for its employees and contractors.
CC6.7.2	Data in-transit is protected through secure (authenticated and encrypted) industry accepted standardized network protocols.
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.	
CC6.8.1	The ability to install applications and software is restricted to authorized personnel. Changes to software configuration parameters are monitored by the system administrator.

Control #	Control Activity Specified by Tokeny
System Operations	
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.	
CC7.1.1	Tokeny maintains updated baseline configurations for its information systems and system components to reflect the current enterprise architecture.
CC7.1.2	Tokeny has implemented a vulnerability management program to detect and remediate system vulnerabilities in software packages used in the Company's infrastructure.
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.	
CC7.2.1	Tokeny maintains updated detection policies, procedures, and tools to identify anomalies or unusual activity on information systems. Potential security incidents are filtered and analyzed based on established detection measures.
CC7.2.2	Detection tools are periodically analyzed by management for effectiveness, and remedial action is taken when necessary.
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.	
CC7.3.1	Tokeny has established an internal ticketing system for tracking potential incidents. Tickets are prioritized based on their impact and severity.
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.	
CC7.4.1	Tokeny maintains an updated Incident Response Program, establishes roles and responsibilities, and includes procedures for containing, mitigating, and ending the threats posed by security incidents and restore operations. The program also includes communication protocols as well as requirements pertaining to understanding the nature of the incident, determining containment strategy, remediating identified vulnerabilities, and communicating remediation activities.
CC7.4.2	Tokeny follows the Incident Response Program by understanding the nature of the incident, determining a containment strategy, remediating identified vulnerabilities and communicating remediation activities.
Please reference *Complementary User Entity Controls (CUECs)* in Section III for additional controls that are to be implemented by user entities.	
CC7.5 – The entity identifies, develops, and implements activities to recover from identified security incidents.	
CC7.5.1	Tokeny follows the Incident Response Program to restore the affected environment to full operation by rebuilding systems, updating software, installing patches, and/or changing configurations, as needed.
CC7.5.2	Information about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are communicated to management and other internal and external parties, as appropriate.
CC7.5.3	After an incident has been resolved and appropriate parties have been notified, a postmortem that includes a root cause analysis and lessons learned is completed. Architectural and/or procedures changes are implemented, when possible, to prevent and detect recurrences of similar incidents. This includes conducting additional training to educate personnel on how to prevent future incidents.
Please reference *Complementary User Entity Controls (CUECs)* in Section III for additional controls that are to be implemented by user entities.	

Control #	Control Activity Specified by Tokeny
Change Management	
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.	
CC8.1.1	Tokeny maintains an updated Change Management Policy that governs the systems development lifecycle, including (1) authorizing system changes prior to development; (2) designing and developing system changes; (3) documenting and tracking changes prior to implementation; (4) testing and approving system changes; (5) deploying changes to production; (6) evaluating the changes against their objectives; and (7) modifying infrastructure, data, software and procedures to remediate identified incidents.
CC8.1.2	Tokeny uses a version control system to manage source code, documentation, release labeling, and other change management tasks.
CC8.1.3	Developers who make changes to the development system are unable to deploy those changes to production without independent approval. An authorized engineer reviews, tests, and approves network configuration changes before the changes are deployed to production. All deployments are logged, including who deployed the change and at what time it was deployed.
CC8.1.4	Changes to the production environment are communicated to affected internal and external stakeholders.

Control #	Control Activity Specified by Tokeny
Risk Mitigation	
CC9.1 – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
Tokeny did not maintain insurance to mitigate the financial impact of business disruptions, including cyber incidents. Exception noted.	
CC9.1.1	Tokeny maintains an updated Business Continuity and Disaster Recovery Plan that guides the organization in how to respond and recover from disruptions in networks, systems, and internal operations. The CTO coordinates and conducts an annual rehearsal of the plan.
Tokeny uses AWS to provide cloud computing and data center hosting services. Please reference *Complementary Subservice Organization Controls (CSOCs*) in Section III for controls that are to be implemented by the subservice organization.	
CC9.2 – The entity assesses and manages risks associated with vendors and business partners.	
CC9.2.1	Tokeny maintains an updated Vendor Management Policy to monitor and ensure service levels and ongoing compliance of existing vendors. The policy outlines roles, responsibilities, and communication protocols around managing vendor relationships and exception handling.
CC9.2.2	Tokeny conducts comprehensive vendor due diligence prior to onboarding a new vendor, as well as on an annual basis for existing vendors. This includes performing a vendor risk assessment and reviewing the SOC 2 / 3 reports, ISO 27001 certifications and/or responses to information security questionnaires.

SECTION V

OTHER INFORMATION PROVIDED BY TOKENY

Management’s Response to Testing Exception

<table>
<tr><th>Control #</th><th>Control Activity Specified by Tokeny</th></tr>
<tr><td colspan="2"><b>CC9.1 – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.</b></td></tr>
<tr><td colspan="2">Tokeny did not maintain insurance to mitigate the financial impact of business disruptions, including cyber incidents. Exception noted.</td></tr>
<tr><td><b>Management’s Response:</b></td><td>Tokeny is in the process of identifying an insurance provider and expects to purchase insurance by September 30, 2023.</td></tr>
</table>