kalderos

System and Organization Controls (SOC) 3 Report

Kalderos, Inc.'s Description of Its Truzo platform

Relevant to Security, Availability, Processing Integrity, and Confidentiality

Throughout the Period November 1, 2024 to October 31, 2025

Table of Contents

Independent Service Auditor's Report

To: Kalderos, Inc. (“Kalderos” or “the Company”)

Scope

We have examined Kalderos’ accompanying assertion titled “Assertion of Kalderos, Inc. Management” (assertion) that the controls within the Company’s Truzo platform were effective throughout the period November 1, 2024 to October 31, 2025, to provide reasonable assurance that Kalderos’ service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, and Confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Kalderos uses subservice organizations for infrastructure and data hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Kalderos, to achieve Kalderos’ service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system 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.

Service Organization’s Responsibilities

Kalderos 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 Kalderos’ service commitments and system requirements were achieved. Kalderos has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Kalderos is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management’s assertion that controls within the system were effective throughout the period to provide reasonable assurance that the Company’s service commitments and system requirements were achieved based on the applicable trust services criteria. 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 management’s assertion

is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve the Company's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve the Company's service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that Kalderos' controls over the Truzo platform were effective throughout the period November 1, 2024 to October 31, 2025, to provide reasonable assurance that Kalderos' service commitments and system requirements were achieved based on the applicable trust services criteria.

Laika Compliance LLC

Arlington, Virginia
December 5, 2025

Assertion of Kalderos, Inc. Management

We, as management of Kalderos, Inc., are responsible for:

- Identifying the Truzo platform and describing the boundaries of the system, which are presented in Attachment A.
- Identifying our principal service commitments and system requirements.
- Identifying the risks that would threaten the achievement of Kalderos' principal service commitments and system requirements that are the objectives of our system, which are presented in Attachment B.
- Identifying, designing, implementing, operating, and monitoring effective controls over the system to mitigate risks that threaten the achievement of the principal service commitments and system requirements.
- Selecting the trust services categories that are the basis of our assertion.

Kalderos uses subservice organizations for infrastructure and data hosting services. The boundaries of the system presented in Attachment A include only the controls of Kalderos and exclude controls of the subservice organizations. However, the description of the boundaries of the system does present the types of controls Kalderos assumes have been implemented, suitably designed, and operating effectively at the subservice organizations. Certain trust services criteria can be met only if the subservice organizations' controls are suitably designed and operating effectively along with the related controls at Kalderos. However, we perform monitoring procedures for the subservice organizations and based on procedures performed, nothing has been identified that prevents us from achieving our specified service commitments and system requirements.

We assert that the controls over the system were effective throughout the period November 1, 2024 to October 31, 2025, to provide reasonable assurance that Kalderos' service commitments and system requirements were achieved based on the criteria relevant to Security, Availability, Processing Integrity, and Confidentiality set forth in the AICPA's TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

Kalderos, Inc.

Attachment A – Truzo platform Overview

SERVICES PROVIDED

Kalderos, Inc. ("Kalderos" or "the Company") has built the Truzo platform to simplify drug discount program compliance for all stakeholders across programs. The platform applies proprietary, internally developed, and supported datasets, algorithms, validations, and machine learning to effectuate drug discount programs proactively to identify and resolve noncompliance where it may have occurred.

The Truzo platform has a few core capabilities under its umbrella:

- **Discount Monitoring** allows providers and manufacturers to work together to identify past non-compliant discounts with industry-leading algorithms trained on the nation's single largest labeled dataset related to duplicate discounts. This discount identification involves collaborative work with thousands of providers, all 50 states, and others to encourage a smooth resolution of noncompliant discounts. This solution can find duplicates within MDRP, 340B, Max Fair Price, and Commercial.
- **Payment Effectuation** is the ability to use a direct discount model (or rebate model) to facilitate payment between the covered entities and the manufacturer. This helps ensure proper discounts reach the right party upfront and prevents duplicate discounts down the line.
- **Truzo platform for Covered Entities** is the provider-facing side of Truzo platform. This is where covered entities submit claims and respond to good faith inquiries.

INFRASTRUCTURE

The Company uses Microsoft Azure, Snowflake, and ShareFile as subservice organizations for infrastructure and data hosting services. However, the Company is responsible for designing and configuring the architecture within Microsoft Azure, Snowflake, and ShareFile to ensure security and resiliency requirements are met. Controls operated by Microsoft Azure, Snowflake, and ShareFile are not included in the scope of this report.

The affected criteria are included below along with the minimum controls expected to be in place at the aforementioned service providers:

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.1	• ShareFile, Microsoft Azure, and Snowflake are responsible for encrypting customer data at rest and in transit within the managed infrastructure to mitigate the risk of unauthorized access to sensitive data.

Criteria	Complementary Subservice Organization Controls (CSOCs)
	• ShareFile, Microsoft Azure, and Snowflake are responsible for implementing access control over the managed infrastructure to mitigate the risk of unauthorized access or privilege escalation.
CC6.4	• ShareFile, Microsoft Azure, and Snowflake are responsible for restricting physical access to their data centers through approval and revocation processes, surveillance and access control mechanisms, periodic reviews of access rights, and retention of monitoring records to mitigate the risk of unauthorized access, intrusion, or physical tampering.
CC6.5	• ShareFile, Microsoft Azure, and Snowflake are responsible for securely decommissioning production assets in their control and ensuring that data is rendered unreadable or unrecoverable through logical deletion, cryptographic erasure, or physical destruction once no longer required, to mitigate the risk of unauthorized recovery of data from retired equipment.
CC6.6	• ShareFile, Microsoft Azure, and Snowflake are responsible for applying security patches to the managed infrastructure as part of routine maintenance to mitigate the risk of vulnerabilities being exploited due to outdated systems. • ShareFile is responsible for implementing network-layer protections and security controls to mitigate the risk of unauthorized system access or data exposure.
CC7.2 A1.2	• ShareFile, Microsoft Azure, and Snowflake are responsible for implementing and maintaining environmental protection measures at their data centers including fire detection and suppression systems, temperature and humidity controls, uninterruptible power supply (UPS) units, backup power sources, and monitoring of environmental conditions to mitigate the risk of outages, equipment failure, or data loss due to environmental hazards or power disruptions.
CC8.1	• ShareFile, Microsoft Azure, and Snowflake are responsible for implementing managed infrastructure changes to mitigate the risk of unauthorized or untested changes affecting system availability, integrity, or confidentiality.
A1.2	• ShareFile, Microsoft Azure, and Snowflake are responsible for managing automated backups of customer data stored within the managed infrastructure to mitigate the risk of data loss or service disruption due to accidental deletion, corruption, or infrastructure failure.

SOFTWARE

Software consists of the programs and software that support the Truzo platform. Software and ancillary software are used to build, support, secure, maintain, and monitor the Truzo platform.

PEOPLE

The Company develops, manages, and secures the Truzo platform via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Customer Success	Responsible for managing customer relationships.
Engineering and Data Management	Responsible for the development, testing, deployment, and maintenance of new code as well as data sourcing and ingestion.
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Finance	Responsible for managing all financial processes and decisions.
Information Security	Responsible for protecting an organization's data, systems, and infrastructure from unauthorized access, misuse, breaches, or other cyber threats.
Product	Responsible for gathering requirements for product features and enhancements.

PROCEDURES

Procedures include the automated and manual procedures involved in the operation of the Truzo platform. Procedures are developed and documented by the respective teams for a variety of processes. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of Truzo platform:

Procedure	Description
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Configuration and Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk and Compliance	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.
Data Backup and Storage	How the Company manages data backups to allow for data restorations to occur if needed.
Business Continuity and Disaster Recovery (BC/DR)	How the Company identifies the steps to be taken in the event of a disaster to help resume business operations.
Data Classification and Handling	How the Company classifies data included in the service and the procedures for handling the data.
Incident Response Plan	How the Company identifies the steps to be taken in the event of a security incident.

DATA

Data refers to transaction streams, files, data stores, tables, and other outputs used or processed by the Truzo platform. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the Truzo platform production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in customer contracts.

The Company has deployed secure methods and protocols for transmission of confidential and sensitive information over public networks. Data stores housing customer data are encrypted at rest.

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Kalderos' controls were designed with the assumption that certain controls would be implemented by user entities (or "customers"). Certain requirements can be met only if complementary user entity controls assumed in the design of Kalderos' controls are suitably designed and operating effectively, along with related controls at Kalderos. Identified complementary user entity controls were included in the service auditor's examination of SOC 2 controls.

Attachment B – Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of Truzo platform. The Master Platform Agreement (MPA) includes the communication of the Company's commitments to its customers.

System requirements are specifications regarding how Kalderos should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the Truzo platform include the following:

Trust Services Category	Service Commitments	System Requirements
Security	Kalderos will implement reasonable technical, administrative, and organizational security measures designed to guard against unauthorized access to customer data maintained by Kalderos.	• Change Management • Encryption Standards • Identity and Access Management • Security Awareness Training • Security Incident Response • Security Monitoring and Reporting • Threat and Vulnerability Management • Vendor Risk Management
Availability	Kalderos will use commercially reasonable efforts to make the online services available 24 hours a day, 7 days a week, except for planned downtime, and any unavailability caused by circumstances beyond Kalderos' reasonable control.	• Business Continuity and Disaster Recovery • Data Backup, Recovery, and Replication

Trust Services Category	Service Commitments	System Requirements
Processing Integrity	Kalderos will implement reasonable technical, administrative, and organizational security measures to process data completely and accurately.	• Data Validation Procedures
Confidentiality	Kalderos will treat all confidential information as confidential and proprietary, and will take reasonable precautions to prevent any unauthorized use or disclosure of confidential information and customer data.	• Data Classification • Data Retention and Disposal • Information Sharing and Confidentiality Standards