System and Organization Controls (SOC) 3

Report on OneSchema AI Inc.'s Data Onboarding System Relevant to Security, Availability, and Confidentiality Throughout the Period July 1, 2024, to June 30, 2025

INSIGHT ASSURANCE

+1 877.607.7727

www.InsightAssurance.com

TABLE OF CONTENTS

SECTION 1:
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON A SOC 3 EXAMINATION

To: OneSchema AI Inc.

Scope

We have examined OneSchema AI Inc.'s ("OneSchema") accompanying assertion titled "OneSchema AI Inc.'s Management Assertion" (assertion) that the controls within the Data Onboarding System (system) were effective throughout the period July 1, 2024, to June 30, 2025, to provide reasonable assurance that OneSchema's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022) in* AICPA, *Trust Services Criteria*.

Service Organization's Responsibilities

OneSchema 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 OneSchema's service commitments and system requirements were achieved. OneSchema has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, OneSchema 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 management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization'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.

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

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 OneSchema'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 OneSchema'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 the effectiveness of 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 the controls within the Data Onboarding System were effective throughout the period July 1, 2024, to June 30, 2025, to provide reasonable assurance that OneSchema's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Insight Compliance LLC

dba Insight Assurance
Tampa, Florida
October 29, 2025

SECTION 2:
ONESCHEMA AI INC.'S MANAGEMENT ASSERTION

ONESCHEMA AI INC.'S MANAGEMENT ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within OneSchema AI Inc.'s ("OneSchema") Data Onboarding System throughout the period July 1, 2024, to June 30, 2025, to provide reasonable assurance that OneSchema's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022),* in AICPA *Trust Services Criteria*. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2024, to June 30, 2025, to provide reasonable assurance that OneSchema AI Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria. OneSchema AI Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2024, to June 30, 2025, to provide reasonable assurance that OneSchema AI Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

OneSchema AI Inc.
October 29, 2025

ATTACHMENT A:
DESCRIPTION OF THE SYSTEM BOUNDARIES

ATTACHMENT A

ONESCHEMA AI INC.'S DESCRIPTION OF THE BOUNDARIES OF THE DATA ONBOARDING SYSTEM

SERVICES PROVIDED

OneSchema Importer is an embeddable CSV importer used by developers to launch CSV import capabilities in a day, instead of months of development time. OneSchema automatically detects and helps correct errors in the data during the import process, so that data is both easier to ingest and higher quality.

The OneSchema system focuses on the following activities for CSV import: automatically fixing user errors during the CSV import process (find-and-replace, auto-fix all errors, deleting in bulk, filtering and navigating errors), exporting to excel with error highlighting, custom data processing with web assembly/webhooks, intelligent mapping, dynamic templates & custom columns, and providing a guided import experience.

INFRASTRUCTURE

OneSchema maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner.

Primary Infrastructure		
Asset	**Type**	**Purpose**
AWS Elastic Compute Cloud (EC2)	AWS	Hosting Provider
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage, upload and download

SOFTWARE

OneSchema is responsible for managing the development and operation of the system. The software supporting the system consists of the applications, programs, and other software components used to build, secure, maintain, and monitor the system. The list of software is shown in the table below.

Primary Software	
System/Application	**Purpose**
GuardDuty	Security application used for automated intrusion detection (IDS)
Datadog	Monitoring application used to provide monitoring, alter, and notification services for OneSchema platform
Vanta	GRC platform
Heroku	Data integration platform
GitHub	Version control
Google Workspace	Identity provider
Amazon Web Services	Cloud Provider
Slack	Communication platform
Asana	Task management
Checkr	Background checking
Sentry	Security system
Rippling	HR System
Stripe	Payment system
Salesforce	CRM
DuploCloud	Infrastructure building system

PEOPLE

The company employs dedicated team members to handle major product functions, including operations and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

OneSchema has a staff organized in the following functional areas:

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

This includes:

- **Chief Executive Officer:** Andrew Luo
- **Chief of Staff:** Sol Chen

Operations: Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

DATA

Data as defined by OneSchema, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured, which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, OneSchema has policies and procedures in place for proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

Data is categorized into the following major types of data used by OneSchema.

Data		
Category	**Description**	**Examples**
Public	Public information is not confidential and can be made public without any implications.	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage. The company must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer

Data		
Category	**Description**	**Examples**
Company data	Information collected and used by the company to operate the business. The company must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

PROCEDURES

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

ATTACHMENT B:
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

OneSchema designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that OneSchema makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that OneSchema has established for the services. The system services are subject to Security, Availability, and Confidentiality commitments established internally for its services.

OneSchema's commitment to customers is communicated through our MSAs, BAAs, and Service Terms & Conditions on the website.

Security Commitments

Security commitments include, but are not limited to, the following

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal

Availability Commitments

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities.
- Operational procedures supporting the achievement of availability commitments to user entities.

Confidentiality Commitments

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties.
- Confidential information must be used only for the purposes explicitly stated in agreements between OneSchema and user entities.