Thoropass™
Assurance

O3 SOLUTIONS

System and Organization Controls (SOC) 3 Report

O3 Insight, Inc.'s Description of the O3 Solution Platform Relevant to Security and Confidentiality Throughout the Period January 1, 2025 to December 31, 2025

TABLE OF CONTENTS

SECTION 1

Independent Service Auditor's Report

Independent Service Auditor's Report

To: O3 Insight, Inc. ("O3 Solutions" or "the Company")

Scope

We have examined O3 Solutions' accompanying assertion titled "Assertion of O3 Insight, Inc. Management" (assertion) that the controls within the Company's O3 Solution Platform were effective throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that O3 Solutions' service commitments and system requirements were achieved based on the trust services criteria relevant to Security 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)*.

O3 Solutions uses a subservice organization 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 O3 Solutions, to achieve O3 Solutions' 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 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.

Service Organization's Responsibilities

O3 Solutions 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 O3 Solutions' service commitments and system requirements were achieved. O3 Solutions has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, O3 Solutions 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 O3 Solutions' 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 O3 Solutions' 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.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement, including the Code of Professional Conduct established by the AICPA, and we have complied with those requirements. In addition, we applied the Statements on Quality Control Standards established by the AICPA, and, accordingly, maintain a comprehensive system of quality control.

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 are 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 over the O3 Solution Platform were effective throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that O3 Solutions' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Thoropass Assurance

Arlington, Virginia
February 5, 2026

SECTION 2

Assertion of O3 Insight, Inc. Management

Assertion of O3 Insight, Inc. Management

We, as management of O3 Insight, Inc., are responsible for:

- Identifying the O3 Solution 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 O3 Solutions' 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.

O3 Solutions uses a subservice organization for infrastructure and data hosting services. The boundaries of the system presented in Attachment A include only the controls of O3 Solutions and excludes controls of the subservice organization. However, the description of the boundaries of the system does present the types of controls O3 Solutions assumes have been implemented, suitably designed, and operating effectively at the subservice organization. Certain trust services criteria can be met only if the subservice organization's controls are suitably designed and operating effectively along with the related controls at O3 Solutions. However, we perform monitoring procedures for the subservice organization 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 January 1, 2025 to December 31, 2025, to provide reasonable assurance that O3 Solutions' service commitments and system requirements were achieved based on the criteria relevant to Security 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,

O3 Insight, Inc.

Attachment A - O3 Solution Platform Overview

Overview of Operations

O3 Insight, Inc. ("O3 Solutions" or "the Company") offers the O3 Solution Platform, a cloud-based digital project management platform purpose-built to support the planning and execution of capital projects, including industrial construction and large-scale project delivery efforts. The platform is designed around industry best practices such as Advanced Work Packaging (AWP) and incorporates modern delivery approaches such as Agile and Lean methodologies to help teams standardize execution, improve visibility, and enhance coordination across project stakeholders.

The O3 Solution Platform supports project activities from early-phase planning through execution and systems completion or start-up, providing tools to organize work into structured packages, track progress, and manage the handoffs required to deliver projects efficiently. The O3 Solution Platform also provides solution modules (e.g., work management/execution capabilities) intended to improve planning, coordination, and field-to-office alignment without requiring customers to fundamentally change their delivery approach.

The platform includes functionality to manage and track work packages and associated actions required for AWP programs and is positioned to support data-driven execution and accountability through centralized project information and structured workflows. Users access the platform through web-based interfaces, and O3 Solutions operates the service as a managed software platform.

Infrastructure

The Company utilizes Microsoft Azure as a subservice organization for infrastructure and data hosting services. By leveraging the resiliency, scalability, and security features of the infrastructure services provided by Microsoft Azure, the Company is able to support current and future demand.

The Company remains responsible for designing, configuring, and maintaining the system architecture within Microsoft Azure to ensure that security and resiliency requirements are met. Controls operated by Microsoft Azure 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 Microsoft Azure.

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.1	Microsoft Azure is responsible for encrypting customer data at rest and in transit within the managed infrastructure to mitigate the risk of unauthorized access to sensitive data. Microsoft Azure is responsible for implementing access control over the managed

Criteria	Complementary Subservice Organization Controls (CSOCs)
	infrastructure to mitigate the risk of unauthorized access or privilege escalation.
CC6.4	Microsoft Azure is responsible for restricting physical access to its 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	Microsoft Azure is responsible for securely decommissioning production assets in its 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	Microsoft Azure is 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.
CC7.2	Microsoft Azure is responsible for implementing and maintaining environmental protection measures at its 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	Microsoft Azure is responsible for implementing managed infrastructure changes to mitigate the risk of unauthorized or untested changes affecting system availability, integrity, or confidentiality.

Software

The Company leverages software components to operate the O3 Solution Platform and deliver services to its customers. These include applications, platforms, and supporting tools used to build, secure, monitor, and maintain the environment. The Company remains responsible for selecting, implementing, and maintaining these software components to ensure that applicable system requirements are met.

People

The Company's personnel are responsible for operating, securing, and supporting the O3 Solution Platform. Personnel perform activities necessary to deliver the Company's services, including governance, operations, customer support, and security-related functions. The Company remains responsible for recruiting, training, and overseeing personnel to ensure that their roles are performed in accordance with applicable policies and requirements.

The in-scope personnel roles and responsibilities are outlined in the table below:

Role/Unit Name	Responsibilities
Customer Success	Responsible for managing and strengthening customer relationships to drive adoption, satisfaction, and retention of products and services.
Engineering	Responsible for the design, development, testing, deployment, and maintenance of software and system components.
Executive Management	Responsible for providing strategic leadership, overseeing company-wide activities, and ensuring organizational goals and objectives are established, communicated, and achieved.
Finance	Responsible for managing the organization's financial resources and processes to support strategic decision-making, compliance, and fiscal sustainability.
Human Resources	Responsible for managing the employee lifecycle, including recruitment, onboarding, role definition, performance management, and terminations, while ensuring compliance with employment laws and policies.
Marketing	Responsible for developing and executing marketing strategies to enhance brand awareness and generate leads.
Sales	Responsible for revenue generation, client acquisition, and management of the sales pipeline.

Procedures

The Company relies on documented automated and manual procedures to govern the operation, security, and support of the O3 Solution Platform. These procedures are maintained in alignment with the Company's Information Security Policy and are reviewed and updated as necessary for changes in the business, but no less than annually. The Company remains responsible for developing, implementing, and maintaining these procedures to ensure they are followed consistently and support the Company's operational and compliance objectives.

The in-scope procedures are outlined in the table below:

Procedure	Description
Access Control	How the Company restricts access to its systems and facilitates, provisions and removes access rights, and prevents unauthorized access.
Asset Management	How the Company tracks and manages its assets, including hardware and

Procedure	Description
	software, to ensure accurate records, compliance with requirements, and protection of resources.
Business Continuity and Disaster Recovery	How the Company identifies the steps to be taken in the event of a disaster to help resume business operations.
Change Management	How the Company identifies, reviews, and implements system changes using a controlled process to prevent unauthorized or untested changes.
Data Classification, Handling, and Retention	How the Company classifies data, establishes requirements for its secure handling and storage, determines retention periods in compliance with requirements, and securely disposes of records when no longer needed.
Incident Management	How the Company detects, reports, responds to, and manages incidents that could affect the operation or protection of the system, in order to minimize impact and support recovery.
Monitoring and Logging	How the Company collects, reviews, and analyzes system activity logs and alerts to detect and respond to unusual or unauthorized activity.
Risk and Vendor Management	How the Company identifies, assesses, and mitigates risks to the system, including risks arising from business disruptions, operations, and the use of vendors and business partners by evaluating, selecting, and monitoring vendors to ensure they meet security and compliance requirements.
Security Awareness and Training	How the Company trains personnel on security and compliance requirements and monitors completion of training activities.
System Operations	How the Company manages and monitors system operations and responds to deviations, including security-related events.

Data

Data refers to the transaction streams, files, data stores, tables, and other outputs used or processed by the O3 Solution Platform. While the Company maintains data necessary for the operation and support of the O3 Solution Platform, customers remain responsible for defining and controlling the data they provide and maintain within the O3 Solution Platform. The Company remains responsible for managing and protecting that data in accordance with its policies, contractual commitments, and applicable regulatory requirements.

Secure data transmission protocols are used to encrypt customer data when transmitted over public networks.

Complementary User Entity Controls (CUECs)

In designing its controls, O3 Solutions management did not identify any CUECs that would be necessary, in combination with controls at O3 Solutions, to provide reasonable assurance that its principal service commitments and system requirements would be achieved. Accordingly, no CUECs are required to achieve the service commitments and system requirements based on the applicable trust services criteria.

User Entity Responsibilities

O3 Solutions' controls related to the O3 Solution Platform are sufficient, in and of themselves, to achieve its principal service commitments and system requirements. Accordingly, no CUECs are required. However, user entities remain responsible for implementing and maintaining their own internal controls to ensure the proper use of the O3 Solution Platform within their environments. These responsibilities are intended to support each user entity's broader control environment, ensure the effective use of the services provided, and help user entities derive benefit from those services. The following responsibilities are illustrative and should not be considered a comprehensive listing:

User entities should:

- Report any material changes to their control environment that may impact the services performed by the Company, in accordance with contractually defined time frames.
- Notify the Company of changes to the authorized user list and vendor security requirements.
- Grant access only to authorized and trained personnel and revoke access timely when access is no longer required.
- Maintain physical security and environmental controls at their facilities and for remote workers.
- Implement controls for managing user IDs and passwords used to access the Company's services.
- Notify the Company of any known or suspected security incidents.

Attachment B - Principal Service Commitments and System Requirements

Service commitments are declarations made by management to customers regarding the performance and security of the O3 Solution Platform. These commitments are communicated to customers through the Company's contractual agreements, policies, and other customer-facing documentation.

System requirements are specifications that define how the O3 Solution Platform is designed and operated in order to meet the Company's principal commitments to customers. These requirements are specified in the Company's policies and procedures, system design documentation, contractual obligations, and applicable laws and regulations.

The Company's principal service commitments and system requirements related to the O3 Solution Platform include the following:

Security Service Commitment and System Requirements

O3 Solutions will take reasonable precautions to protect customer data and other confidential information in accordance with the reasonable standard of care.

To meet this commitment, the Company has established system requirements, including:

- Change Management
- Encryption Standards
- Identity and Access Management
- Network Security and Segmentation
- Policy Management and Governance
- Security Awareness Training
- Security Incident Response
- Security Monitoring and Reporting
- Threat and Vulnerability Management
- Vendor Risk Management

Confidentiality Service Commitment and System Requirements

O3 Solutions will not use proprietary information except in the performance of services and will not divulge any proprietary information to any third party, unless permitted.

To meet this commitment, the Company has established system requirements, including:

- Data Classification
- Data Retention and Secure Disposal

- Encryption of Confidential Data
- Information Sharing and Confidentiality Standards