A-LIGN

InEight, Inc.

Type 2 SOC 3

2023

INEIGHT

A-LIGN.COM

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

June 1, 2022 to May 31, 2023

Table of Contents

SECTION 1

ASSERTION OF INEIGHT, INC. MANAGEMENT

ASSERTION OF INEIGHT, INC. MANAGEMENT

June 15, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within InEight, Inc.'s ('InEight' or 'the Company') SaaS and Project Management Services System throughout the period June 1, 2022 to May 31, 2023, to provide reasonable assurance that InEight's 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*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "InEight, Inc.'s Description of Its SaaS and Project Management Services System throughout the period June 1, 2022 to May 31, 2023" 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 June 1, 2022 to May 31, 2023, to provide reasonable assurance that InEight's service commitments and system requirements were achieved based on the trust services criteria. InEight'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 "InEight, Inc.'s Description of Its SaaS and Project Management Services System throughout the period June 1, 2022 to May 31, 2023".

InEight uses Microsoft Azure ('Azure' or 'subservice organization') to provide data center and cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at InEight, to achieve InEight's service commitments and system requirements based on the applicable trust services criteria. The description presents InEight's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of InEight'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 to achieve InEight's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of InEight's controls.

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 June 1, 2022 to May 31, 2023 to provide reasonable assurance that InEight's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of InEight's controls operated effectively throughout that period.

Scott Workman

Scott Workman
Chief Administrative Officer
InEight, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR’S REPORT

To InEight, Inc.:

Scope

We have examined InEight, Inc.’s (‘InEight’ or ‘the Company’) accompanying assertion titled “Assertion of InEight, Inc. Management” (assertion) that the controls within InEight’s SaaS and Project Management Services System were effective throughout the period June 1, 2022 to May 31, 2023, to provide reasonable assurance that InEight’s 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*, in AICPA *Trust Services Criteria*.

InEight uses Azure to provide data center and cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at InEight, to achieve InEight’s service commitments and system requirements based on the applicable trust services criteria. The description presents InEight’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of InEight’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 InEight, to achieve InEight’s service commitments and system requirements based on the applicable trust services criteria. The description presents InEight’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of InEight’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.

Service Organization’s Responsibilities

InEight 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 InEight’s service commitments and system requirements were achieved. InEight has also provided the accompanying assertion (InEight assertion) about the effectiveness of controls within the system. When preparing its assertion, InEight 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 AICPA. 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 the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- 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

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

Independence and Ethical Responsibilities

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

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 suitability of the design and operating 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 InEight’s SaaS and Project Management Services System were suitably designed and operating effectively throughout the period June 1, 2022 to May 31, 2023, to provide reasonable assurance that InEight’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of InEight’s controls operated effectively throughout that period.

The SOC logo for Service Organizations on InEight’s website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of InEight, user entities of InEight's SaaS and Project Management Services during some or all of the period June 1, 2022 to May 31, 2023, business partners of InEight subject to risks arising from interactions with the SaaS and Project Management Services, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
June 15, 2023

SECTION 3

INEIGHT, INC.’S DESCRIPTION OF ITS SAAS AND PROJECT MANAGEMENT SERVICES SYSTEM THROUGHOUT THE PERIOD JUNE 1, 2022 TO MAY 31, 2023

OVERVIEW OF OPERATIONS

Company Background

InEight was founded in 1989 and is a leading developer of construction project management software that enables contractors, engineers, and owners to overcome their greatest project pain points. InEight's solutions span every stage of the project life cycle from design to estimate and field execution to turnover. The solutions give project stakeholders real-time information and insights needed to minimize risks, improve operational efficiency, control project costs, and make educated decisions.

Based in Scottsdale, Arizona, InEight has offices in Omaha, Nebraska; Melbourne, Australia; Colombo, Sri Lanka. InEight, an ISO registered company, is a subsidiary of Kiewit Corporation (Kiewit). Kiewit, through its subsidiaries, is one of North America's largest construction and engineering organizations.

Description of Services Provided

InEight is a leader in project management software, with solutions spanning every phase of delivery from design through estimate, field execution and turnover. InEight has solutions for every phase beginning with owner's early planning and engineering, and through construction and turnover.

The InEight Suite allows owners to choose what best meets their needs today and easily add on in the future. InEight's solution comprises a suite of purpose-built, integrated products. This integrated suite ensures stakeholders share a single version of project truth across the stages of the project life cycle, enabling them to make accurate and timely decisions. This modular and integrated product approach facilitates the cross-product sharing of users, roles, documents, reports and other project data, minimizing data rework and duplicate data entry. InEight's software solutions seamlessly integrate with other systems, including enterprise resource planning, scheduling and model data.

Principal Service Commitments and System Requirements

InEight designs its processes and procedures related to Project Suite to meet its objectives for its SaaS and Project Management Services System. Those objectives are based on the service commitments that InEight makes to user entities, the laws and regulations that govern the provision of SaaS services, and the financial, operational, and compliance requirements that InEight has established for the services. The SaaS and Project Management Services System of InEight is subject to the security and privacy requirements of ISO 27001/2013.

Security commitments to user entities are documented and communicated in service level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of Project Suite that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

InEight establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in InEight's system 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 how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of Project Suite.

Components of the System

Infrastructure

Primary infrastructure used to provide InEight's SaaS and Project Management Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Azure	Cloud	Web Application
Azure	Cloud	Structured Query Language (SQL) Database
Azure	Cloud	Data Bus
Active Directory	Windows	Centralized domain management

Software

Primary software used to provide InEight's SaaS and Project Management Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Internet Information Services	Windows	Web Application
SQL	Microsoft	Database
.NET	Microsoft	Custom Program
Cisco AnyConnect	Not applicable	Virtual Private Network (VPN)

People

InEight has a staff of approximately 500 employees organized in the following functional areas:

- Corporate: Executives, senior operations staff, and company administrative support staff, such as legal, training, accounting, human resources (HR), sales, and marketing. These individuals manage business planning, sales and marketing strategies and other support functions need for daily business operations
- Development and Operations (DevOps): Staff that administers the Azure scheduling and administration of changes, code deployments, infrastructure support and customer bug fix deployments
- Information Technology (IT): Product Support, IT infrastructure, IT networking, IT system administration, software tool development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom:
    - The product support group provides technical assistance to InEight software users
    - The infrastructure, networking, and systems administration staff typically has no direct use of Project Suite Rather, it supports InEight's IT infrastructure, which the Development Team uses. A DevOps administrator will deploy the releases of Project Suite and other software into the production environment

- The software development staff develops and maintains the custom software for InEight. This includes Project Suite, supporting utilities, and the external websites that interact with Project Suite. The staff includes software developers, database administration, software quality assurance, and technical writers
- The information security staff supports Project Suite indirectly by monitoring internal and external security threats and maintaining current antivirus software
- The Internal IT staff maintains the inventory of IT assets
- DevOps manage the user interfaces for Project Suite. This includes processing environment build and standup requirements for each customer
- Network Security personnel maintain the voice communications environment, provide user support to InEight, and resolve communication problems. This group does not directly use Project Suite, but it provides infrastructure support as well as disaster recovery assistance

Data

Data, as defined by InEight, constitutes the following:

- SQL Data stored in Azure
- Transaction data
- Customer input
- System files
- Error logs

Transaction processing is initiated by the entry of project data to the user websites, or it may be bulk imported at system origination. Once the data is entered or imported into the system it is maintained in the SQL database or in the Customer Relationship Management (CRM) system. This data is maintained in the project container for the duration of the project. The interaction and data manipulation is controlled by the customer and the roles and permissions are established by the customers admin in the dedicated Azure instance and the Application roles and permissions module.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to InEight policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any InEight team member.

Physical and Environmental Security

The in-scope system and supporting infrastructure is hosted by Azure. As such, Azure is responsible for the physical security controls for the in-scope system.

Logical Access

Upon hire, employees are assigned to a position in the HR management system. Prior to the employees' start date, the HR management team creates an onboarding ticket for each new employee. The internal ticketing system assigns the tasks to create user IDs and access to be granted. The ticket is used by the security team to monitor and audit appropriate roles assignments.

On a quarterly basis, application owners review access to their applications. Access listings are requested by security and distributed to the application owners via the internal ticketing system. Application owners review the listings and indicate the required changes in the internal ticket. The record is routed back to the access administrators for processing.

Upon an employee’s termination of employment, the HR team automatically generates an offboarding ticket. This ticket is routed to the access administrators for deletion. In addition, terminated employees turn over their access cards/IDs during their exit interview. These cards are then sent to the executive assistant for return and reprograming by the building manager.

On an annual basis, managers review roles assigned to their direct reports. This is done as part of the annual performance and review process. Managers review direct reports and assign roles.

Computer Operations - Backups

Customer data is backed up and monitored by DevOps personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

Backup infrastructure and on-site backup media are physically secured in locked cabinets and/or caged environments within the third-party data centers. The backup infrastructure resides on private networks logically secured from other networks. Backup restoration tests are performed on an annual basis.

Contracted customer off-site media rotations are logged and maintained within an enterprise ticket management system. A third-party provider that specializes in off-site media rotation has been contracted to perform off-site media rotation services for clients that select this as part of the backup service. The ability to recall backup media from the third-party off-site storage facility is restricted to authorized DevOps personnel.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network. Business continuity and disaster recovery plans are developed and updated on an annual basis and are tested on an annual basis.

InEight monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches SLAs. InEight evaluates the need for additional infrastructure capacity in response to the growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Azure resource pools
- Disk storage
- Backup Vault Space
- Network bandwidth

Change Control

InEight maintains documented Systems Development Life Cycle (SDLC) 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 (UAT) 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. Designated Employees approve changes prior to migration to the production environment and document the approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers. File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal Internet protocol (IP) addresses. Administrative access to the firewall is restricted to authorized employees. Also, an intrusion prevention system (IPS) is utilized to analyze network events and report possible or actual network security breaches.

Redundancy is built into the system infrastructure supporting the workplace and support systems to help ensure that there is no single point of failure that includes firewalls, routers, and switches. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted annually to measure the security posture of a target system or environment. The InEight security team uses an accepted industry standard penetration testing methodology specified by InEight. The InEight security team approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the security team attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by the security team on a quarterly basis in accordance with InEight policy. The InEight security team uses industry standard scanning technologies and a formal methodology specified by InEight. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an annual basis. Scans are performed during non-peak windows. Tools requiring installation in the InEight system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a multi-factor authentication system tied to the Active Directory.

Boundaries of the System

The scope of this report includes the SaaS and Project Management Services System performed in the Scottsdale, Arizona; Omaha, Nebraska; Melbourne, Australia; Colombo, Sri Lanka facilities.

This report does not include the data center and cloud hosting services provided by Azure at multiple facilities.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common Criteria/Security and Confidentiality criterion were applicable to the InEight SaaS and Project Management Services System.

Subservice Organizations

This report does not include the data center and cloud hosting services provided by Azure at multiple facilities.

Subservice Description of Services

Azure provides data center and cloud hosting services, which includes implementing physical security controls to protect the housed in-scope systems. Controls include, but are not limited to, visitor sign-ins, required use of badges for authorized personnel, and monitoring and logging of the physical access to the facilities.

Complementary Subservice Organization Controls

InEight's services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the Trust Services Criteria related to InEight's services to be solely achieved by InEight control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of InEight.

The following subservice organization controls should be implemented by Azure to provide additional assurance that the Trust Services Criteria described within this report are met:

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.

InEight management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as SLAs. In addition, InEight performs monitoring of the subservice organization controls, including the following procedures:

- Testing controls performed by vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

InEight's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to InEight's services to be solely achieved by InEight control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of InEight's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to InEight.
2. User entities are responsible for notifying InEight of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of InEight services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize InEight services.
6. User entities are responsible for providing InEight with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying InEight of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.