Invevo®

Report on Description of Invevo Limited's Business Process Management System and the Suitability of the Design and Operating Effectiveness of Controls for the Period November 1, 2023 to October 31, 2024 Relevant to Security

SOC 2®

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Invevo Limited:

Scope
We have examined Invevo Limited's ("Invevo" or "Company") accompanying description of its Business Process Management System titled "Description of Invevo Limited's Business Process Management System" throughout the period November 1, 2023 to October 31, 2024 ("description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Invevo's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("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*).

Invevo uses subservice organizations to provide managed services in support of the Business Process Management system. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Invevo, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Invevo's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Invevo'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.

Service organization's responsibilities
Invevo 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 Invevo's service commitments and system requirements were achieved. Invevo has provided the accompanying assertion titled "Invevo's Management Assertion" ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Invevo 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 and operating effectiveness 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 and operated effectively 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 the description of a service organization's system and the suitability of the design and operating effectiveness 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 or did not operate effectively
- 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
- Testing the operating effectiveness of controls stated in the description 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 other 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 users may consider important to meet their informational needs.

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.

Description of tests of controls
The specific controls we tested and the nature, timing and results of those tests are presented in section VI.

Basis for qualified opinion
The service organization states in its description that it has controls in place for the documentation, testing and approval of changes to the application(s) and supporting infrastructure and associated content covering emergency change requests and the communication of changes both internally and externally. However, as noted in section VI of the description of tests and controls and results, controls related to the documentation, testing and approval of changes to the application(s) and supporting infrastructure and associated content covering emergency change requests and the communication of changes both internally and externally, could not be validated during the period November 1, 2023 through October 31, 2024. As a result, controls were not operating effectively to achieve trust services criterion 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."

Qualified opinion
In our opinion, except for the matters discussed in the preceding paragraph, in all material respects, based on the criteria described in Invevo's assertion in section II of this report.

Opinion
In our opinion, in all material respects,

a. The description presents Invevo's Business Process Management System that was designed and implemented throughout the period November 1, 2023 to October 31, 2024, in accordance with the description criteria.

b. Except for matters described in the following paragraph, the controls stated in the description were suitably designed throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Invevo's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if subservice organizations applied the complementary controls assumed in the design of Invevo's controls throughout that period.

c. As noted in section VI, controls related to the documentation, testing and approval of changes to the application(s) and supporting infrastructure and associated content covering emergency change requests and the communication of changes both internally and externally, could not be validated during the period November 1, 2023 to October 31, 2024.

As a result, controls were not operating effectively to achieve trust services criterion 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."

Restricted use

This report, including the description of tests of controls and results thereof in section VI, is intended solely for the information and use of Invevo, user entities of Invevo's Business Process Management System during some or all of the period of November 1, 2023 to October 31, 2024, business partners of Invevo subject to risks arising from interactions with the Business Process Management 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 service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, 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.

IS Partners, LLC

IS Partners, LLC
Dresher, Pennsylvania
July 18, 2025

II. INVEVO'S MANAGEMENT ASSERTION

We have prepared the accompanying description of Invevo Limited's ("Invevo" or "Company") Business Process Management System titled "Description of Invevo Limited's Business Process Management System" throughout the period November 1, 2023 to October 31, 2024 ("description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"). The description is intended to provide report users with information about the Business Process Management System that may be useful when assessing the risks arising from interactions with Invevo's system, particularly information about system controls that Invevo 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 section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Invevo uses subservice organizations to provide managed services in support of the Business Process Management system. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Invevo, to achieve Invevo's service commitments and system requirements based on the applicable trust services criteria. The description presents Invevo's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Invevo's controls. The description does not disclose the actual controls at the subservice organization.

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

a) The description presents Invevo's Business Process Management System that was designed and implemented throughout the period of November 1, 2023 to October 31, 2024, in accordance with the description criteria.

b) Except for matters described in the following paragraph, the controls stated in the description were suitably designed and operated effectively throughout the period November 1, 2023 to October 31, 2024 to provide reasonable assurance that Invevo's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if subservice organizations applied the complementary controls assumed in the design of Invevo's controls throughout that period.

c) As noted in section VI, controls related to the documentation, testing and approval of changes to the application(s) and supporting infrastructure and associated content covering emergency change requests and the communication of changes both internally and externally, could not be validated during the period November 1, 2023 to October 31, 2024. As a result, controls were not operating effectively to achieve trust services criterion 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."

III. DESCRIPTION OF INVEVO LIMITED'S BUSINESS PROCESS MANAGEMENT SYSTEM

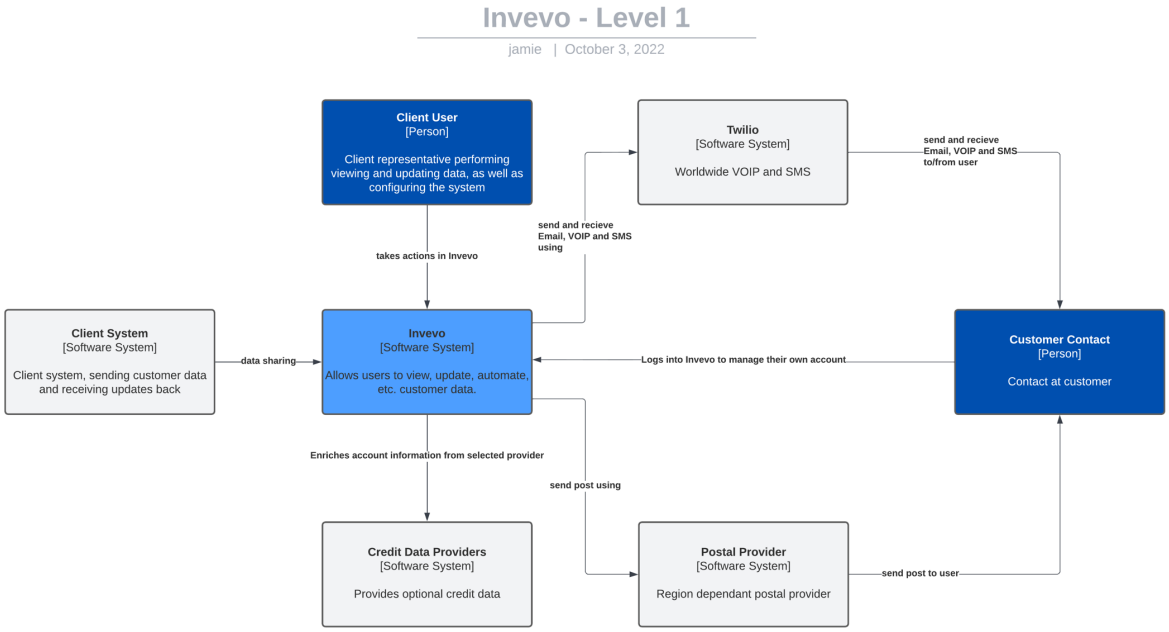
Company Overview

Invevo Limited provides a SaaS based product suite, which simplifies the credit collection process for clients. Invevo's clients are based all around the globe, but are more prominent in the UK. Invevo Limited was founded in 2020 to provide financial technology to all sectors.

Services Provided

Invevo is a multi-user, multi-tenanted SaaS platform focused on risk management and collections. It provides the following features:

- Intelligent Automation of communication and updating, sharing and enriching customer data.
- Customer self-service portal.
- Integrated credit reporting.
- Data insights.
- Customer workspaces and dashboards.



Principal Service Commitments and System Requirements

Invevo designs its processes and procedures related to the platform to meet its objectives for its services. Those objectives are based on the service commitments that Invevo makes to user entities, the laws and regulations that govern the provision of services, and the financial, operational, and compliance requirements that Invevo has established for the services. The services of Invevo are subject to the security and privacy requirements of GDPR.

Security commitments to user entities are documented and communicated in Service Level Agreements ("SLA") 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 the system 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
- Various preventive IT controls are in place to protect against the introduction of malicious software
- Internal monitoring is conducted over the control environment internally for governance of client data
- Mechanisms are utilized for continuous communication to internal and external stakeholders as needed.
- Use of encryption technologies to protect customer data both at rest and in transit

Invevo establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Invevo'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 the platform.

Components of the System
The system is comprised of the following five components:

- Infrastructure
- Software
- People
- Procedures
- Data

Infrastructure

The platform runs on Azure Kubernetes Services. Invevo employees access the application through their company-supplied laptop or through an approved 'bring your own device' model.

Data is stored in Azure, primarily using Kafka streams backed by Azure Storage Accounts, or in an Azure Managed Instance database depending on type of data.

Software

The platform is developed and maintained by Invevo's in-house software engineering group. The software engineering group enhances and maintains the platform.

The platform receives information in real time or through frequent intra-daily batches depending on client configuration. The information is immediately stored in the database of choice and is accessible via relevant read model. The information can be retrieved, reviewed, and reported as needed.

The Invevo web interface is a multiuser, web-based application that helps users configure automated tasks, check information in an ad-hoc manner (through searching, or reports) and view tasks they have been assigned. This website also allows users to update certain information about customers they manage. It also provides some specific performance reports to help users monitor their customers, and their teams' customers.

People

Invevo employs approximately 30 members of staff in the following business areas:

- ***Sales***. Provides remote walkthroughs of the Invevo application on the Demo Platform. Access is only provided to this area of the platform.
- **Account Management**. Provides day to day client relations activities, and assists with the support requests handled by Product Support.
- ***Project Management***. Responsible for guiding the evolution of the Invevo platform and prioritizing features and projects. Work closely with multiple teams within the business and with external clients.
- ***Marketing***. Our marketing team does not interact with the Invevo application.
- ***Engineering***. Junior and Senior Developers, deploy new versions of our application to demo, then production environments. They support Invevo's IT infrastructure, which is used by the software. The software development staff develops and maintains the custom software for Invevo. This includes the application, supporting utilities, and the external applications that interact with the application, like Azure. The staff includes software developers, application administration and software quality assurance. Engineering also assist with technical project implementation.
- ***Service Delivery***. Service Management and Product Support provide day to day support for clients. Taking inbound support requests via email, which are managed and progressed within the ITSM System 'Autotask'. Whilst technical capabilities are present, the Product Support Team do not make any environmental changes to the system. Configuration changes are only made on the user profile layer.
- ***Management***. Directors and senior operations staff. Their responsibilities include legal matter, compliance, internal audits, training, contracting, accounting, finance, human resources, and supplier relations.

Data

Data, as defined by Invevo, constitutes the following:

- Customer data
- Transaction data
- Payment data
- Internal users

- Lookup data (e.g. currencies, exchange rates)
- System logs

Processing is initiated either by a user action, a data change, or on a timer. This can then trigger further actions (e.g. an email to a customer reminding them payment is due, which may drive the customer to dispute the payment raising another task for a user)

Output reports are available on the website, in CSV or embedded in an email. The availability of these reports is limited by job function. Reports delivered externally will only be sent using a secure method (encrypted email, secure FTP, or secure websites) via approved mechanisms and to approved users. Invevo uses Transport Layer Security to encrypt email exchanges.

Data Backup and Recovery
Invevo uses Azure data replication and backup features to keep its data secure and replicated globally. Access to backup devices, scheduling utilities, systems, and media is restricted to authorized personnel.

Processes and Procedures

Management has developed and communicated to all business functions, procedures to restrict logical access to the Invevo application. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls)

Disclosure of Security Incidents

Invevo diligently responds to alerts received from various monitoring tools deployed at the perimeter of the network, within the network and applications. Invevo did not have any security incidents significant enough to trigger external communications during the period November 1, 2023 to October 31, 2024.

IV. OTHER RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION SYSTEMS, AND MONITORING CONTROLS

The security category and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security criteria are included in section 4 of this report. Although the applicable trust services criteria and related controls are included in section 4, they are an integral part of Invevo description of the our platform.

Control Environment

Management Philosophy
Invevo's control environment reflects the philosophy of senior management concerning the importance of security of medical transportation and logistics data and information. Invevo's Security Steering Committee meets quarterly and reports to the board annually. The committee, under the direction of Invevo board, oversees the security activities of Invevo. The committee members are from each of the business lines. The committee is charged with establishing overall security policies and procedures for Invevo. The importance of security is emphasized within Invevo through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, Invevo has taken into consideration the relevance of controls to meet the relevant trust criteria.

Security Management
Invevo has a dedicated information security team consisting of a CTO and Head of Service Delivery, who is responsible for management of information security throughout the organization. They hold positions on the Security Steering Committee and maintain security credentials and are required to annually sign and acknowledge their review of the information security policies. They are responsible for developing, maintaining, and enforcing Invevo's information security policies. The information security policy is reviewed annually by the CTO and Head of Service Delivery.

As the information security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings or through system alerts.

During annual security training and awareness programs, management ensures communication of the latest security policies as well as written job descriptions for security management.
Additionally, management is responsible for ensuring service agreements are current for third parties and for updating the annual IT risk assessment.

Security Policies
The following security policies and related processes are in place for Invevo:

- Data classification and business impact assessment
- Selection, documentation, and implementation of security controls
- Assessment of security controls
- User access authorization and provisioning
- Removal of user access
- Monitoring of security controls
- Security management

Tugboat Logic has been implemented to enhance the workflow and approval process in support of the policies. This application enables tracking of:

- changes to data classification;
- additions, modifications, or deletions of users;
- changes to authority levels in access approvals;
- tests of new security components prior to installation; and
- reviews of significant security monitoring events.

Personnel Security
Background checks are performed on new information security employees, who are also required to review and acknowledge their receipt of relevant security policies. The new positions are supported by job descriptions. Once employed, employees are subject to Invevo's procedures for accessing systems and sanctions for violating Invevo's information security policy. Employees are instructed to report potential security incidents to the help desk.

Invevo's Service agreement instructs user entities and transportation providers to notify their respective account representative if they become aware of a possible security breach.

System Account Management
Invevo has implemented role-based security to limit and control access within the application. Employees are granted logical and physical access to in-scope systems based on documented approvals by appropriate management personnel. Invevo's clients and suppliers all require approval for access by the Account Management team and named approver contact client/vendor side. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel. User access is reviewed quarterly to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts.

The human resources department provides IT personnel with an employee termination document at the point of notice being received, or contract termination taking place. IT reconciles the termination report with current access privileges to determine if access has been appropriately removed or disabled. Dormant network accounts are disabled after 90 days of inactivity, and dormant Invevo accounts are disabled after 180 days of inactivity.

Administrative access to Active Directory, Unix, and Invevo servers and databases is restricted to authorized employees.

Unique user identification numbers, names, and passwords are required to authenticate all users to the Invevo, as well as to the facility services, transportation provider, member services, and client reporting websites. Password parameters consist of the following:

- Passwords contain a minimum of six characters, including one non-alphanumeric character.
- Passwords expire every 120 days for non-privileged accounts and 60 days for privileged accounts.
- Log-on sessions are terminated after three failed log-on attempts.
- Users cannot reuse the last three passwords (five passwords for privileged accounts).

Risk Assessment Process

Invevo regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security based on the applicable trust services criteria set forth in TSP section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The information security team assesses security risks on an ongoing basis. This is done through regular management meetings with IT personnel, reviewing and acting upon security event logs, performing vulnerability assessments, and conducting a formal annual IT risk assessment in conjunction with the company-wide risk assessment.

An IT strategic plan is developed annually by the CTO and is communicated to and approved by senior management and the Security Steering Committee. As part of this plan, strategic IT risks affecting the organization and recommended courses of action are identified and discussed.

Senior management, as part of its annual information security policy review, considers developments in technology and the impact of applicable laws and regulations on Invevo's security policies.

Changes in security threats and risks are reviewed by Invevo, and updates to existing control activities and information security policies are performed as necessary.

Information and Communication Systems

Invevo has an information security policy to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

Invevo uses checklists to help facilitate the upload of user (rider or member) information, such as encounter data, trip report, and client complaints, to the appropriate repository (for example, a portal or secure FTP folder) in accordance with the user's instructions.

Change Management
Invevo has a formalized change management process in place, which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed. The IT management team meets weekly to review and schedule changes to the IT environment.

Emergency changes follow the formalized change management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented.

Changes to infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments.

Invevo has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.

Invevo uses a standardized server build checklist to help secure its servers, and it conducts monthly vulnerability assessments to identify potential system vulnerabilities. Patches are applied regularly in accordance with Invevo patch management process.

Problem Management
Security incidents and other IT-related problems are reported to the help desk. Issues are tracked using a help desk ticket and monitored until resolved.

Monitoring Controls

In addition to the daily oversight, monthly vulnerability assessments, and regular pen tests, management provides further security monitoring through the internal engineering department, which performs periodic audits and monitors security alerts.

System Monitoring
The Engineering team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system ("IDS") and intrusion prevention system ("IPS") alerts, vulnerability assessment reports, and operating system event logs. These alerts and notifications are reviewed every working day. Additionally, administrators receive alerts when a user requests access to secure resources.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of how the Business Process Management System is used to provide the service during the period from November 1, 2023 through October 31, 2024.

V. SUBSERVICE ORGANIZATIONS

Invevo Limited uses a subservice organization to perform certain functions that support the delivery of services. The scope of this report does not include the controls and related Trust Services Criteria at the subservice organization. The following is a description of the services provided by the subservice organization and the controls that are expected to be implemented:

Subservice Organization	Services Provided
Microsoft Azure	*Managed Cloud Provider*
Confluent	*Managed Kafka Provider*
Elastic NV	*Managed Elastic Provider*

The following table presents controls that are assumed to be implemented by the subservice organization, which Invevo Limited has identified as necessary to achieve certain Trust Services Criteria stated in the system description.

Trust Services Criterion	Complementary Subservice Organization Controls
CC 6.4 – 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.	• Physical access to data centers is approved by an authorized individual. • Physical access is revoked within 24 hours of the employee or vendor record being deactivated. • Physical access to data centers is reviewed on a quarterly basis by appropriate personnel. • Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations. Access to server locations is managed by electronic access control devices.
CC 6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	• Physical access to data centers is approved by an authorized individual. • Physical access is revoked within 24 hours of the employee or vendor record being deactivated. Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.

Monitoring of Subservice Organization

There are several risks that are outside of Invevo's control ownership and are categorized under the internal controls of the subservice organizations. Invevo identifies these risks and ensures that the subservice organizations include controls to help mitigate these risks as they relate to the Company. Invevo Limited requests a SOC 2 report and any other due diligence documents that may be appropriate as required, at least once per year. The management team reviews all documents and reports from the subservice organizations.

Controls that do not fall under the subservice organization's responsibility are incorporated into Invevo Limited's policies and procedures, and if warranted, reflected in Invevo's SOC 2 report.

VI. INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
AA1	Unique user IDs and passwords are required in order to gain access to the Company's infrastructure (Microsoft Azure) supporting the application, including - Minimum 8 Characters - Complexity Requirements for 1 special character, 1 numeric character, 1 lowercase character, 1 uppercase character	Obtained and inspected the Password Policy and determined the Password Policy states unique user IDs and passwords are required in order to gain access to Invevo's infrastructure and passwords must be at a minimum of 8 characters and met complexity standards. Obtained and inspected the system configuration and determined that password configurations were configured as per the Password Policy.	No exceptions noted.	CC6.1
AA2	The Invevo application maintains a default password configuration (for end-users not utilizing Single Sign-On), which includes an eight character minimum.	Obtained and inspected the password configurations and determined that the Invevo application maintained a default password configuration (for end-users not utilizing Single Sign-On), which included an eight character minimum.	No exceptions noted.	CC6.1
AA3	Multi-factor authentication ("MFA") is enforced for user accounts with administrative access to the organization's infrastructure (Microsoft Azure).	Obtained and inspected the multi-factor authentication configurations and determined that MFA was enforced for user accounts with administrative access to the organization's infrastructure (Microsoft Azure).	No exceptions noted.	CC6.1
AC1	Access to in-scope system components (the Invevo application and its underlying infrastructure) requires a documented access request and approval from management prior to access provisioning.	For a sample of new hires during the audit period, obtained and inspected evidence of access approvals to determine that access to in-scope system components required a documented access request and approval from management prior to access provisioning.	No exceptions noted.	CC6.1; CC6.2; CC6.3

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
AC2	Management utilizes an employee termination checklist to ensure that the termination process is consistently executed, and access is revoked for terminated employees in a timely manner.	Obtained and inspected termination tickets for a selection of terminated employees during the audit period and determined that management utilized an employee termination checklist to ensure that the termination process was consistently executed, and access was revoked for terminated employees in a timely manner.	No exceptions noted.	CC6.1; CC6.2; CC6.3; CC6.4
AC3	Access to a privileged account on the Company's infrastructure (Microsoft Azure) or application is restricted to authorized IT personnel based on a role-based access scheme.	Obtained and inspected the Access Control Policy and determined privileged access is to be restricted to authorized IT personnel based on a role-based access scheme. Obtained and inspected the list of users with administrative access to the system and determined that access to privileged accounts on Invevo's infrastructure (Microsoft Azure) was restricted to authorized IT personnel based on a role-based access scheme.	No exceptions noted.	CC6.3; CC6.8
AC4	Management performs a quarterly user access review for in-scope system components to ensure that access is restricted appropriately. Access is modified or removed in a timely manner based on the results of the review.	Obtained and inspected the user access reviews for a selection of quarters during the audit period and determined that management performed a quarterly user access review for in-scope system components to ensure that access was restricted appropriately. Additionally, determined that access was modified or removed in a timely manner based on the results of the review.	No exceptions noted.	CC6.2; CC6.3

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
AC5	System components are configured such that the organization and its customers' access is appropriately segmented from other tenant users.	Obtained and inspected evidence of segmented tenants and determined system components were configured such that the organization and its customers' access was appropriately segmented from other tenant users.	No exceptions noted.	CC6.1
AC6	Access to promote changes to production is restricted to authorized personnel based on job responsibilities.	Obtained and inspected the list of users who have access to promote changes to production to determine that access to promote changes to production was restricted to authorized personnel based on job responsibilities. Obtained and inspected approval tickets for a selection of changes during the audit period to determine that changes were promoted to production by authorized personnel.	No exceptions noted.	CC6.3; CC8.1
AT1	The organization utilizes Tugboat Logic platform to manage its Information Security policies and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.	Obtained and inspected the policies and procedures from the company intranet to determine that policy and procedure documents relating to security, confidentiality, and availability are made available to employees and reviewed on an annual basis.	No exceptions noted.	CC1.4; CC2.2; CC5.3
AT2	Employees are required to complete an information security and awareness training annually.	Obtained and inspected evidence of training completion for a selection of employees and determined employees were required to complete an information security and awareness training annually.	No exceptions noted.	CC1.4; CC2.2

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
AT3	Relevant organizational employees are trained on the functional use of the application to understand their roles and responsibilities as part of the onboarding process.	Obtained and inspected evidence of onboarding training completion for a selection of new hires during the audit period and determined that relevant organizational employees were trained on the functional use of the application to understand their roles and responsibilities as part of the onboarding process.	No exceptions noted.	CC2.1; CC2.3
AT4	The organization has developed documentation and user guides that describe relevant system components as well as the purpose and design of the system. These documents are made available to both internal and external users and updated as needed.	Obtained and inspected documentation and user guides and determined that Invevo has developed documentation and user guides that describe relevant system components as well as the purpose and design of the system. Obtained and inspected evidence of the Company intranet and system and determined documentation was made available to both internal and external users and updated as needed.	No exceptions noted.	CC2.1; CC2.2; CC2.3
CM1	A formal change management process exists that governs changes to the applications and supporting infrastructure. The process document is reviewed by IT management on an annual basis and updated as needed.	Obtained and inspected Invevo's Change Management policy and determined that a formal change management process existed that governs changes to the applications and supporting infrastructure. Additionally, the process document was reviewed by IT management on an annual basis and updated as needed.	No exceptions noted.	CC6.8; CC8.1

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
CM2	Emergency change requests are documented and subject to the standard change management process but at an accelerated timeline. Prior to initiating an emergency change, appropriate approval is obtained and documented.	Obtained and inspected the Change Management policy to determine that documentation is in place to require appropriate approval prior to implementing an emergency change that is documented. Observed and inspected emergency change tickets to determine that emergency changes are documented and subjected to the standard change management process however, evidence from within the audit period was unable to be provided.	Exception noted. - For two (2) of the three (3) sampled emergency changes, documentation of approval was not provided.	CC8.1

Management's Response to the Exception Identified in Control CM2: Invevo does not operate a separate or distinct "emergency change" process. Our platform architecture and continuous integration/deployment capabilities are designed to support rapid, secure, and standardized changes at any time — including those that might be deemed "emergency" in other environments.

Invevo deploys on-demand through our standard, audited change management pipeline, which includes: peer-reviewed and approved pull requests ("PRs"), CI/CD checks and validations, audit trails within our version control and deployment tooling, traceability of all changes via integrated ticketing and source control systems. This approach eliminates the need for bypassed or expedited change paths, as even high-priority fixes are subject to the same rigor and governance controls as all other changes. Given this structure:

- We do not distinguish emergency changes from regular changes.
- As such, no special designation or filtering for emergency PRs exists.
- PRs relevant to incidents are linked contextually but not separately tagged.

This design is intentional and reflects our focus on agility without compromising control or auditability. Specific PRs were not provided as "emergency changes," are in no way different to standard PRs, and we have hundreds of repos with thousands of commits.

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
CM3	A formal system development life cycle ("SDLC") methodology is established that governs the development, acquisition, implementation, and maintenance of application development and enhancement projects.	Obtained and inspected Invevo's Software Development Policy and determined that a formal SDLC methodology was established that governed the development, acquisition, implementation, and maintenance of application development and enhancement projects.	No exceptions noted.	CC8.1
CM4	Changes that affect the functionality and security of the system components are communicated to internal and external users.	Observed and inspected change tickets to determine that changes that affect the functionality and security of the system components were communicated to internal and external users, however, evidence from within the audit period was unable to be provided.	Exception noted. - For two (2) of the three (3) sampled emergency changes, documentation of approval was not provided.	CC2.2; CC8.1

Management's Response to the Exception Identified in Control CM4: Invevo currently communicates changes that may impact functionality or security through its Account Management team, who maintain regular touchpoints with both internal stakeholders and external clients. These updates are delivered during scheduled calls and are tailored to the operational and strategic context of each customer. Invevo recognizes the importance of consistent and scalable communication and are in the process of evolving toward a marketing-led approach. This future state will include:

- Proactive distribution of formal release notes
- Structured customer communications for significant updates
- Internal enablement materials to ensure alignment across teams

This planned enhancement will improve transparency, ensure consistent messaging, and provide greater clarity to users about system updates that may impact them.

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
CM5	Changes to the application(s) and supporting infrastructure are documented, tested and approved prior to implementation into the production environment in accordance with the change management process.	Obtained and inspected the Change Management policy to determine that a change management process exists and documented. Observed and inspected change tickets to determine that changes to the application(s) and supporting infrastructure were documented, tested and approved prior to implementation into the production environment in accordance with the change management process, however, evidence from within the audit period was unable to be provided.	Exception noted. - For twenty-one (21) of the twenty-five (25) sampled changes, documentation of testing and approval was not provided.	CC8.1

Management's Response to the Exception Identified in Control CM5: At Invevo, all changes to the application and infrastructure are governed by the documented Change Management Policy, which is enforced through tightly integrated tooling and workflows. While traditional Zendesk-based ticketing is not used for feature development, all feature and infrastructure changes are rigorously tracked and managed through:

- Monday.com and Linear (current systems of record for planning and tracking)
- Azure DevOps (historically used prior to full migration)

Our development workflow ensures that:

- All work must be associated with a tracked ticket, which is linked directly to its corresponding pull request ("PR")
- No code can be merged without a fully reviewed and approved PR
- This PR process includes peer review, CI checks, and validation gates, all of which are aligned with our change management and security policies

This integrated approach ensures traceability, testing, and approval of changes prior to deployment into production, even if these actions are not captured in Zendesk. The absence of Zendesk tickets for changes during the audit period is not indicative of a gap in controls, but rather reflects the structure and efficiency of our tooling ecosystem. Supporting artifacts from Monday.com, Linear, and Git-based PR systems can be made available on request to demonstrate adherence to our policy.

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
CM6	Changes to application and system infrastructure are developed and tested in a separate development or test environment before implementation.	Obtained and inspected screenshot evidence of test environments to determine that changes to application and system infrastructure were developed and tested in a separate development or test environment before implementation.	No exceptions noted.	CC8.1
CR2	Weekly full-system and daily incremental back-ups are performed using an automated system and replicated to an offsite location. Backups are monitored for failure using an automated system.	Obtained and inspected the backup configurations to determine that weekly full-system and daily incremental back-ups were performed using an automated system and replicated to an offsite location. Additionally, determined that backups were monitored for failure using an automated system.	No exceptions noted.	CC7.4
CR6	Disaster recovery plans (including restoration of backups) have been developed and tested annually. Test results are reviewed and consequently contingency plans are updated.	Obtained and inspected the most recent disaster recovery test and determined that disaster recovery plans (including restoration of backups) have been developed and tested annually. Obtained and inspected the Disaster Recovery Plan and determined that test results were reviewed and consequently contingency plans were updated.	No exceptions noted.	CC7.4
DS2	Production data is prohibited to be used outside of the production environment by policy.	Obtained and inspected the Software Development Policy and determined that production data was prohibited to be used outside of the production environment by policy.	No exceptions noted.	CC6.7; CC8.1

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
DS4	Formal data retention and disposal policy and procedure are in place to guide the secure retention and disposal of information.	Obtained and inspected the Data Retention and Disposal Policy and determined that formal data retention and disposal policy and procedure were in place to guide the secure retention and disposal of information.	No exceptions noted.	CC6.5
HR1	Information security roles and responsibilities of employees, contractors, and the organization are stated in contractual agreements.	Obtained and inspected contracts for a selection of personnel during the audit period and determined information security roles and responsibilities of employees, contractors, and the organization were stated in contractual agreements.	No exceptions noted.	CC1.3; CC1.5; CC2.2; CC2.3
HR2	Job descriptions that document the objectives of the role, responsibilities, reporting lines, employee qualifications and other requirements are made available to the employees. Job descriptions are reviewed and updated annually or in case of significant changes.	Obtained and inspected the job description documentation to determine that job descriptions that document the objectives of the role, responsibilities, reporting lines, employee qualifications and other requirements were made available to the employees that are reviewed on an annual basis or as needed based on significant changes.	No exceptions noted.	CC1.3; CC1.4
HR3	Organization has established an organization chart that defines organizational roles, reporting lines, and authorities as it relates to development, quality assurance, and security operations of its services. The organization structure is reviewed and updated in case of significant changes.	Obtained and inspected Invevo's organization chart and determined that Invevo had established an organization chart that defined organizational roles, reporting lines, and authorities as it relates to development, quality assurance, and security operations of its services. Additionally, determined that the organization structure was reviewed and updated in case of significant changes.	No exceptions noted.	CC1.3

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
HR4	The organization has a process in place to evaluate the competency of employees and identify their development needs on an annual basis.	Obtained and inspected employee performance evaluations for a selection of employees during the audit period and determined Invevo had a process in place to evaluate the competency of employees and identify their development needs on an annual basis.	No exceptions noted.	CC1.4; CC1.5
HR5	The organization has a formal training plan in place for the employees and meets annually to identify relevant training needs to support in scope-systems.	Obtained and inspected evidence that background checks were conducted for a selection of new hires during the audit period and determined that new employees were subjected to background checks prior to joining the organization.	No exceptions noted.	CC1.4
HR6	New employees are subjected to background checks prior to joining the organization.	Per inquiry with management, background checks were not available for new hires.	Exception noted - For the eleven (11) new hires sampled, records of criminal background checks completed were not maintained.	CC1.4
Management's Response to the Exception Identified in Control HR6: At the time of hiring certain employees, a full background check process had not yet been implemented. Invevo has since established a robust background screening procedure, which now includes a DBS check, verification of previous employment references, and a review of publicly available social media activity where appropriate. This process is now embedded into the onboarding workflow for all new hires moving forward. Invevo is also reviewing existing employees to identify whether retroactive screening is appropriate.				

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
IM1	The organization provides an external-facing support system that allows users to report incidents, complaints, issues, and any other challenge through an appropriate channel. Reported incidents are addressed by the organization's support staff in a timely manner.	Observed and inspected Invevo's support page and determined that Invevo provided an external-facing support system that allowed users to report incidents, complaints, issues, and any other challenge through an appropriate channel. Obtained and inspected support incidents for a selection of incidents reported during the audit period and determined that reported incidents were addressed by Invevo's support staff in a timely manner.	No exceptions noted.	CC2.3; CC7.4
IM2	Notifications regarding confirmed data breaches are provided to affected data subjects, regulators, and other parties (as applicable) within an acceptable timeframe to meet the organization's privacy and confidentiality commitments.	Obtained and inspected Invevo's Incident Management Policy and determined that notifications regarding confirmed data breaches are to be provided to affected data subjects, regulators, and other parties (as applicable) within an acceptable timeframe to meet the organization's privacy and confidentiality commitments. Inquired with management regarding data breach notification and determined that there were identified instances of data breaches during the audit period.	Unable to conclude.	CC7.3; CC7.4

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
IM3	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated as required.	Obtained and inspected Invevo's Security Incident Management Policy and determined that a formal incident management process had been established and implemented which required incidents to be tracked, documented and resolved in a complete, accurate and timely manner. Additionally, determined that the process document was reviewed by management on an annual basis and updated as required.	No exceptions noted.	CC2.2; CC2.3; CC7.2; CC7.3; CC7.4
IM4	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with the formal incident management process.	For a sample of incidents during the audit period, obtained and inspected incident tickets to determine that all incidents related to security were logged, tracked and communicated to affected parties while being resolved in a timely manner in accordance with the formal incident management process.	No exceptions noted.	CC7.2; CC7.3; CC7.4; CC7.5
IM5	Management has established defined roles and responsibilities to oversee the implementation of security policies including incident response.	Obtained and inspected the Information Security Policy and determined that management had established defined roles and responsibilities to oversee security. Obtained and inspected the Incident Management Policy and determined that management had established defined roles and responsibilities to oversee the implementation of incident response.	No exceptions noted.	CC7.4

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
IM6	Management incorporates lessons learned from ongoing incident response activities into incident response procedures on an ongoing basis.	For sample for incidents during the audit period, obtained and inspected evidence of lessons learned to determine that management incorporated lessons learned from ongoing incident response activities into incident response procedures on an ongoing basis.	No exceptions noted.	CC7.3; CC7.4; CC7.5
OM1	The organization maintains an inventory of production information assets including details on asset ownership, data classification and location. The asset inventory listing is reviewed and updated by management on an as-needed basis.	Obtained and inspected the asset inventory list to determine that an asset inventory list is maintained of production information assets including details on asset ownership, data classification and location that is reviewed and updated on an as-needed basis.	No exceptions noted.	CC2.1; CC6.1
OM2	The Board of Directors provides corporate oversight, strategic direction, and review of management for the Company. The Board of Directors meets on a quarterly basis for oversight on internal controls, operations and business objectives.	For a sample of quarters during the audit period, obtained and inspected evidence of Board of Directors meetings to determine that the Board of Directors provided corporate oversight, strategic direction, and review of management for Invevo. Additionally, determined that the Board of Directors met on an quarterly basis for oversight on internal controls, operations and business objectives.	No exceptions noted.	CC1.2; CC2.2; CC2.3
OM3	The Board of Directors understand and acknowledge the Board of Directors' contractual responsibilities and accept their oversight responsibilities in relation to established requirements and expectations.	Obtained and inspected the Board of Directors Charter and determined that the Board of Directors understood and acknowledged the Board of Directors' contractual responsibilities and accepted their oversight responsibilities in relation to established requirements and expectations.	No exceptions noted.	CC1.2

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
OM4	The organization has defined a Code of Conduct and Ethics and reviews them annually.	Obtained and inspected Invevo's Employee Code of Conduct and Invevo's Corporate Ethics Policy and determined that Invevo has defined a Code of Conduct and Corporate Ethics Policy. Additionally, determined that the Code of Conduct and Ethics was reviewed annually.	No exceptions noted.	CC1.1
OM5	The organization has established Acceptable Use and Corporate Ethics Policies which are both reviewed/updated on an annual basis by Executive Management. As part of the formal onboarding process, all employees are required to sign indicating their agreement and acknowledgment of the Acceptable Use and Corporate Ethics Policies and re-sign annually thereafter or in the event of any significant revisions.	Obtained and inspected signed agreements for a selection of new hires and active employees during the audit period and determined Invevo had signed agreements in place to acknowledge the Acceptable Use and Corporate Ethics Policies. Obtained and inspected evidence of policy review and determined that the Acceptable Use and Corporate Ethics Policies were both reviewed/updated on an annual basis by Executive Management.	No exceptions noted.	CC1.1; CC1.5; CC2.2
OM6	The management team of the organization meets at quarterly intervals to discuss operations, issues relating to internal controls and delivery on key performance metrics.	For a sample of quarters during the audit period, obtained and inspected management meeting minutes to determine that the management team of the organization met at quarterly intervals to discuss operations, issues relating to internal controls and delivery on key performance metrics.	No exceptions noted.	CC1.2; CC2.2; CC4.1; CC5.1; CC5.3

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
OM7	The organization has formal agreements in place with customers which acknowledges their compliance on security, confidentiality and privacy commitments.	For one (1) of the sampled three (3) customers selected, the signed customer agreement was not a maintained by the Company.	Exception noted - For one (1) of the three (3) customers selected, IS Partners determined that a formal agreement with the customer was not retained.	CC2.3
Management's Response to the Exception Identified in Control OM7: This particular customer is using Invevo's legacy system and was originally onboarded under a different trading name prior to the current contractual and onboarding standards. As a result, a formal customer agreement under the current entity is not in place for this account. However, Invevo is reviewing all legacy customer relationships to align them with the current agreement and control requirements.				
OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.	Obtained and inspected the internal control assessment and determined that Invevo documented their internal controls and continuously monitored its effectiveness. Additionally, determined that an assessment over the effectiveness and efficiency of the internal controls, processes and policies was reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.	No exceptions noted.	CC1.5; CC2.1; CC4.1; CC4.2; CC5.1; CC5.2; CC5.3
OM9	The organization has established communication channels that allow employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.	Obtained and inspected Invevo's Code of Conduct and determined that Invevo had established communication channels that allowed employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.	No exceptions noted.	CC1.1; CC1.5; CC2.2; CC2.3

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
OM10	New customer contracts or modifications to existing customer contracts and end-user license agreements ("EULA") are reviewed annually by Management to ensure security and confidentiality commitments are met.	For a sample of customers during the audit period, obtained and inspected customer contracts to determine that new customer contracts or modifications to existing customer contracts and end-user license agreements (EULA) were reviewed annually by Management to ensure security and confidentiality commitments were met. Per inquiry with management, one (1) out of three (3) customer contracts were not signed or updated since acquiring the contract.	Exception noted. One (1) out of three (3) sampled customers did not have an updated signed contract.	CC2.3
Management's Response to the Exception Identified in Control OM10: This particular customer is using Invevo's legacy system and was originally onboarded under a different trading name prior to the current contractual and onboarding standards. As a result, a formal customer agreement under the current entity is not in place for this account. However, Invevo is reviewing all legacy customer relationships to align them with the current agreement and control requirements.				
RM1	Management maintains insurance coverage through an external service provider against major financial risks for the overall business.	Obtained and inspected Invevo's certificate of insurance coverage and determined that management-maintained insurance coverage through an external service provider against major financial risks for the overall business.	No exceptions noted.	CC9.1
RM2	Management performs a formal risk assessment (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.	Obtained and inspected the risk assessment to determine that management performed a formal risk assessment on an annual basis that identified risks and mitigation strategies were documented and implemented by executive management.	No exceptions noted.	CC3.1; CC3.2; CC3.3; CC3.4; CC9.1

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
SO1	Antivirus software is in place to prevent or detect and act upon the introduction of unauthorized or malicious software.	Observed and inspected the antivirus software configuration and determined that antivirus software was in place to prevent or detect and act upon the introduction of unauthorized or malicious software.	No exceptions noted.	CC6.8
SO2	Infrastructure has been configured to automatically scale the capacity and performance needs of the systems.	Obtained and inspected the automatic capacity and performance monitoring configurations and determined that infrastructure was configured to automatically scale the capacity and performance needs of the systems.	No exceptions noted.	CC7.2
SO3	Baseline configurations are retained within the configuration management tool for rollback capability anytime an approved configuration change is made.	Obtained and inspected the baseline configurations and determined that baseline configurations were retained within the configuration management tool for rollback capability anytime an approved configuration change was made.	No exceptions noted.	CC6.8; CC7.1; CC8.1
SO4	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to production access keys is restricted to authorized individuals.	Obtained and inspected cloud provider key configurations to determine that the cloud provider key management service encrypts data at rest as well as stores and manages encryption keys. Obtained and inspected a list of users with access to production access keys to determine that access to production access keys was restricted to authorized individuals.	No exceptions noted.	CC6.1; CC6.6; CC6.7
SO5	Customer data is encrypted at rest (stored and backup) using strong encryption technologies.	Obtained and inspected system configurations and determined that customer data was encrypted at rest using strong encryption technologies.	No exceptions noted.	CC6.1; CC6.7

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
SO6	Encryption technologies are used to protect communication and transmission of data over public networks and between systems.	Obtained and inspected the encryption configuration and determined that encryption technologies were used to protect communication and transmission of data over public networks and between systems.	No exceptions noted.	CC6.1; CC6.6; CC6.7
SO8	Intrusion detection or prevention systems are used to provide continuous monitoring of the Company's network and to protect potential security breaches.	Obtained and inspected the intrusion detection and prevention system configurations and determined that an intrusion detection or prevention system was used to provide continuous monitoring of Invevo's network and to protect potential security breaches.	No exceptions noted.	CC6.6; CC7.2
SO9	A log management process has been formalized to make sure that access to change the log configuration and access to modify logs is restricted.	Obtained and inspected the Logging and Monitoring Policy and determined that a log management process has been formalized. Obtained and inspected a listing of users with administrative access and determined that access to change the log configuration and access to modify logs was restricted.	No exceptions noted.	CC7.1
SO10	A centralized mobile device management solution has been deployed to all mobile devices to enforce built-in detective and preventive security controls.	Obtained and inspected the Mobile Device Management policy to determine that documentation is in place to implement a central mobile device management system. Per inquiry with management, there was not a central MDM system in place during the audit period.	Exception noted.	CC6.8

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
Management's Response to the Exception Identified in Control SO10: While a centralized Mobile Device Management ("MDM") solution was not fully deployed during the audit period, Invevo had established and enforced baseline mobile and endpoint access controls using Microsoft's native device management capabilities. This included: • Conditional Access Policies to restrict connections to Invevo systems from unauthorized or non-compliant devices • Integration with Microsoft 365 security configurations to block access from unmanaged endpoints As part of Invevo's ongoing commitment to strengthening endpoint security, we are in the process of deploying Microsoft Intune to establish a fully featured MDM platform. This will enhance Invevo's ability to enforce device compliance, implement more granular control policies, and maintain comprehensive visibility over all corporate endpoints. The Mobile Device Management Policy reflects this roadmap and Invevo's evolving security posture, and we expect full deployment and operationalization of Intune in the near term.				
SO11	A formal network diagram outlining boundary protection mechanisms (e.g. firewalls, IDS, etc.) is maintained for all network connections and reviewed annually by IT management.	Obtained and inspected the network diagram and determined that a formal network diagram outlining boundary protection mechanisms was maintained for all network connections and reviewed annually by IT management.	No exceptions noted.	CC6.1; CC6.6
SO12	A patch management process exists to confirm that operating system level vulnerabilities are remediated in a timely manner. In addition, production servers are scanned to test patch compliance on a quarterly basis.	Obtained and inspected the Patch Management Process and configurations and determined that a patch management process existed to confirm that operating system level vulnerabilities were remediated in a timely manner. Obtained and inspected scans for a selection of quarters during the audit period and determined that production servers were scanned to test patch compliance on a quarterly basis.	No exceptions noted.	CC7.5

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
SO13	A penetration test is performed on an annual basis to identify security exploits. Issues identified are classified according to risk, analyzed and remediated in a timely manner.	Obtained and inspected the annual penetration test and determined that a penetration test was performed on an annual basis to identify security exploits. Additionally, determined that issues identified were classified according to risk, analyzed and remediated in a timely manner.	No exceptions noted.	CC4.1; CC7.1
SO14	Logging is enabled to monitor activities such as administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT management and issues identified are resolved in a timely manner through the incident management process.	Obtained and inspected the SIEM configurations to determine that logging was enabled to monitor activities such as administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles. For a sample of incidents during the audit period, obtained and inspected tickets to determine that automated alerts were configured to notify IT management and issues identified were resolved in a timely manner through the incident management process.	No exceptions noted.	CC7.1; CC7.2
SO15	System firewalls are configured on the application gateway and production network to limit unnecessary ports, protocols and services. Firewall rules are reviewed on an annual basis by IT management.	Obtained and inspected the firewall configuration and annual review and determined that system firewalls were configured on the application gateway and production network to limit unnecessary ports, protocols and services. Additionally, determined firewall rules were reviewed on an annual basis by IT management.	No exceptions noted.	CC6.6; CC7.2

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
SO16	The IT team continuously monitors system capacity and performance through the use of monitoring tools to identify and detect anomalies that could compromise availability of the system operations. Incident management process is invoked for confirmed events and anomalies.	Obtained and inspected the monitoring tool configuration to determine that the IT team continuously monitored system capacity and performance through the use of monitoring tools to identify and detect anomalies that could compromise availability of the system operations. Inquired with management regarding confirmed events or anomalies to determine that no instances of confirmed events or anomalies were identified during the audit period.	No exceptions noted.	CC7.2
SO17	Vulnerability scan is performed on a quarterly basis to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.	For a sample of quarters during the audit period, obtained and inspected vulnerability scans to determine that vulnerability scan were performed on a quarterly basis to identify threats and vulnerabilities to the production systems.	No exceptions noted.	CC3.2; CC4.1; CC7.1; CC7.4
VM1	Third-party contractors working on behalf of the organization are required to sign an agreement outlining the standard code of conduct, security and confidentiality requirements.	Obtained and inspected the service agreements for a selection of contractors during the audit period and determined that third-party contractors working on behalf of the organization were required to sign an agreement outlining the standard code of conduct, security and confidentiality requirements.	No exceptions noted.	CC1.1; CC2.2

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
VM2	On an annual basis, management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.	Obtained and inspected evidence of annual SOC report reviews and determined that management performed reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.	No exceptions noted.	CC1.4; CC4.1; CC6.4; CC9.2
VM3	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors on an annual basis. Corrective actions are taken as required based on the results of the assessments.	Obtained and inspected the Vendor Management policy to determine that a documented vendor management process had been implemented. For a sample of vendors during the audit period, obtained and inspected the vendor risk assessments to determine that management performed risk assessments of potential new vendors and evaluates the performance of existing vendors on an annual basis. Additionally, determined that corrective actions were taken as required based on the results of the assessments.	No exceptions noted.	CC1.4; CC3.2; CC3.4; CC9.2
VM4	Vendor management process has been implemented that includes security procedures to be followed in case of vendor terminations.	Obtained and inspected the Vendor Management Policy and determined that a vendor management process had been implemented that included security procedures to be followed in case of vendor terminations. Inquired with management and determined there were no vendors terminated during the audit period.	No exceptions noted. Unable to conclude.	CC9.2

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
WS1	Security software (firewall, anti-virus and anti-spam) is installed and enabled on all workstations.	Obtained and inspected evidence from Invevo's workstations and determined that security software (firewall, anti-virus and anti-spam) was installed and enabled on workstations.	No exceptions noted.	CC6.8
WS2	Disk encryption and system passwords are enabled across all organization workstations.	Obtained and inspected the workstation configurations to determine that disk encryption and system passwords were enabled across organization workstations.	No exceptions noted.	CC6.1; CC6.7
WS3	A patch management process exists to confirm that operating system level vulnerabilities for workstations are remediated in a timely manner. In addition, workstations are scanned to test patch compliance on a quarterly basis.	Obtained and inspected the Patch Management policy to determine that documentation is in place to require a patch management process be implemented to confirm that operating system level vulnerabilities for workstations were remediated in a timely manner. Per inquiry with management, there was no implemented patch management configurations in place during the audit period.	Exception noted.	CC7.5

Key	Control Activity	Tests of Operating Effectiveness	Results	Criteria Reference Links
Management's Response to the Exception Identified in Control WS3: Invevo's production infrastructure architecture does not rely on traditional, full operating system virtual machines. Instead, the workloads run in containerized environments orchestrated by Azure Kubernetes Service ("AKS") — a Microsoft-managed platform. As a result: • Operating system-level patching is handled by Microsoft as part of the underlying AKS node management. • Invevo does not have direct access to, nor manage, base operating system patching for these nodes. Invevo's focus is on maintaining application-level security and container image integrity, which includes: • Regular base image updates for containers • CI/CD pipelines that scan for vulnerabilities • Controlled promotion of tested and signed images into production This cloud-native model is aligned with modern DevOps practices and Invevo's Patch Management Policy reflects this architectural design, emphasizing container security, image lifecycle governance, and dependency vulnerability remediation rather than manual OS-level patching.				

AICPA Trust Services Criteria Reference Table

Criteria	Criteria Description	Control Activity
CC1.0 Control Environment		
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	OM4; OM5; OM9; VM1
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	OM2; OM3; OM6
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	HR1; HR2; HR3
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	AT1; AT2; HR2; HR4; HR5; HR6; VM2; VM3
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	HR1; HR4; OM5; OM8; OM9
CC2.0 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.	AT3; AT4; OM1; OM8
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.	AT1; AT2; AT4; CM4; HR1; IM3; OM2; OM5; OM6; OM9; VM1
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	AT3; AT4; HR1; IM1; IM3; OM2; OM7; OM9; OM10
CC3.0 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.	RM2
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.	RM2; SO17; VM3
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	RM2

Criteria	Criteria Description	Control Activity
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	RM2; VM3
CC4.0 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.	OM6; OM8; SO13; SO17; VM2
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 the board of directors, as appropriate.	OM8
CC5.0 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.	OM6; OM8
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	OM8
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.	AT1; OM6; OM8
CC6.0 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.	AA1; AA2; AA3; AC1; AC2; AC5; OM1; SO4; SO5; SO6; SO11; WS2
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.	AC1; AC2; AC4
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.	AC1; AC2; AC3; AC4; AC6

Criteria	Criteria Description	Control Activity
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	AC2; VM2
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	DS4
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	SO4; SO6; SO8; SO11; SO15
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.	DS2; SO4; SO5; SO6; WS2
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.	AC3; CM1; SO1; SO3; SO10; WS1
CC7.0 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.	SO3; SO9; SO13; SO14; SO17
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.	IM3; IM4; SO2; SO8; SO14; SO15; SO16
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.	IM2; IM3; IM4; IM6
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.	CR2; CR6; IM1; IM2; IM3; IM4; IM5; IM6; SO17
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	IM4; IM6; SO12; WS3
CC8.0 Change Management		

Criteria	Criteria Description	Control Activity
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.	AC6; CM1; CM2; CM3; CM4; CM5; CM6; DS2; SO3
CC9.0 Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	RM1; RM2
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	VM2; VM3; VM4

VII. ADDITIONAL INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITOR

Selection Criteria for Specific Tests
In selecting tests of the operating effectiveness of controls, we considered the

a) nature of the items being tested,
b) the types and adequacy of available evidential matter,
c) the nature of the trust services criteria to be achieved, and
d) the expected efficiency and effectiveness of the test.

Types and Descriptions of the Tests of Operating Effectiveness
Various testing methods are used to assess the operating effectiveness of controls during the examination period. The table below describes the various methods that were employed in testing the operating effectiveness of controls that are in place at the Company.

Testing Procedure	Description
Inquiry	Inquired of appropriate personnel and corroborated with management.
Observation	Observed the application or existence of the specific control as represented.
Inspection	Inspected documents and records indicating performance of the control.
Reperformance	Reperformed the control, or processing of the application control, for accuracy of its operation.

Procedures for Assessing Completeness and Accuracy of Client-Provided Information ("CPI")
For tests of controls requiring the use of CPI (for example, controls requiring system-generated populations for sample-based testing), we performed a combination of the following procedures where possible, based on the nature of the CPI, to address the completeness, accuracy, and integrity of the data or reports used:

a) inspect the source of the CPI,
b) inspect the query, script, or parameters used to generate the CPI,
c) tie data between the CPI and the source, and/or
d) inspect the CPI for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

In addition to the above procedures, for tests of controls requiring management's use of CPI in the execution of the controls (for example, periodic reviews of user access listings), we inspected management's procedures to assess the validity of the CPI source and the completeness, accuracy, and integrity of the data or reports.