A-LIGN

# ContractPod Technologies Inc.

# Type 2 SOC 1

2024

ContractPodAi

# REPORT ON MANAGEMENT’S DESCRIPTION OF CONTRACTPOD TECHNOLOGIES INC.’S SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

**Pursuant to Statement on Standards for Attestation Engagements No. 18 (SSAE 18) Type 2**

**October 1, 2023 to September 30, 2024**

# Table of Contents

# SECTION 1

# ASSERTION OF CONTRACTPOD TECHNOLOGIES INC.’S MANAGEMENT

# ASSERTION OF CONTRACTPOD TECHNOLOGIES INC. MANAGEMENT

October 7, 2024

We have prepared the description of ContractPod Technologies Inc.'s ('ContractPodAI' or 'the Company') AI Based Contract Management Solutions Services System for processing user entities' transactions entitled "Description of ContractPod Technologies Inc.'s AI Based Contract Management Solutions Services System" throughout the period October 1, 2023 to September 30, 2024, (description) for user entities of the system during some or all of the period October 1, 2023 to September 30, 2024, and their user auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

ContractPodAI uses Microsoft Azure ('Azure' or 'subservice organization') for cloud hosting services. The description includes only the control objectives and related controls of ContractPodAI and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by ContractPodAI in the description can be achieved only if complementary subservice organization controls assumed in the design of ContractPodAI's controls are suitably designed and operating effectively, along with the related controls at ContractPodAI. The description does not extend to controls of the subservice organization.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of ContractPodAI controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

a. The description fairly presents the AI Based Contract Management Solutions Services System made available to user entities of the system during some or all of the period October 1, 2023 to September 30, 2024, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

   i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including:

      (1) the types of services provided including, as appropriate, the classes of transactions processed.

      (2) the procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities.

      (3) the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

      (4) how the system captures significant events and conditions, other than transactions.

      (5) the process used to prepare reports and other information for user entities.

(6) services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.

(7) the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the service organization’s controls.

(8) other aspects of our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

ii. includes relevant details of changes to the service organization’s system during the period covered by the description.

iii. does not omit or distort information relevant to the scope of the AI Based Contract Management Solutions Services System, while acknowledging that the description is prepared to meet the common needs of broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the AI Based Contract Management Solutions Services System that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2023 to September 30, 2024, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of ContractPodAI’s controls throughout the period October 1, 2023 to September 30, 2024. The criteria we used in making this assertion were that:

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Anurag Malik

Anurag Malik
President/CTO
ContractPod Technologies Inc.

# SECTION 2

# INDEPENDENT SERVICE AUDITOR’S REPORT

## INDEPENDENT SERVICE AUDITOR'S REPORT

To: ContractPod Technologies Inc.

*Scope*

We have examined ContractPodAI's description of its AI Based Contract Management Solutions Services System for processing user entities' transactions entitled "Description of ContractPod Technologies Inc.'s AI Based Contract Management Solutions Services System" throughout the period October 1, 2023 to September 30, 2024, (description) and the suitability of the design and operating effectiveness of ContractPodAI's' controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Assertion of ContractPod Technologies Inc.'s Management" (assertion). The controls and control objectives included in the description are those that management of ContractPodAI believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the AI Based Contract Management Solutions Services System that are not likely to be relevant to user entities' internal control over financial reporting.

ContractPodAI uses Azure for cloud hosting services. The description includes only the control objectives and related controls of ContractPodAI and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by ContractPodAI can be achieved only if complementary subservice organization controls assumed in the design of ContractPodAI are suitably designed and operating effectively, along with the related controls at ContractPodAI. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of ContractPodAI's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls.

*Service Organization's Responsibilities*

In Section 1 of this report, ContractPodAI has provided their assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. ContractPodAI is responsible for preparing the description and their assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

*Service Auditor's Responsibilities*

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

We conducted our examination 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, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2023 to September 30, 2024. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved
- Evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in their assertion

*Independence and Ethical Responsibilities*

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

*Inherent Limitations*

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements, and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become inadequate or fail.

*Description of Tests of Controls*

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4.

*Opinion*

In our opinion, in all material respects, based on the criteria described in ContractPodAI's assertion,

a. The description fairly presents the AI Based Contract Management Solutions Services System that was designed and implemented throughout the period October 1, 2023 to September 30, 2024.
b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2023 to September 30, 2024 and subservice organizations and user entities applied the complementary user entity controls contemplated in the design of ContractPodAI's controls throughout the period October 1, 2023 to September 30, 2024.

c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2023 to September 30, 2024, if complementary subservice organization and user entity controls assume in the design of ContractPodAI’s controls operated effectively throughout the period October 1, 2023 to September 30, 2024.

*Restricted Use*

This report, including the description of tests of controls and results thereof in Section 4 is intended solely for the information and use of ContractPodAI, user entities of ContractPodAI’s AI Based Contract Management Solutions Services System during some or all of the period October 1, 2023 to September 30, 2024, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities’ financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
October 7, 2024

# SECTION 3

# DESCRIPTION OF CONTRACTPOD TECHNOLOGIES INC.’S AI BASED CONTRACT MANAGEMENT SOLUTIONS SERVICES SYSTEM

## OVERVIEW OF OPERATIONS

### Company Background

ContractPodAI was founded in 2012 with the mission to make contract management more accessible to corporate in-house legal teams and with the aim of eliminating data entry for the corporate lawyer.

Laying original claim to the phrase ‘by lawyers for lawyers’ the platform was created as an affordable out of the box, end to end tool, featuring repository, contract generation and third-party review functionality. Since going live in 2015, the platform has been assisting legal departments at large scale corporations across the globe to digitally transform their contract management function.

### Description of Services Provided

*Complete End-To-End Fully Comprehensive Functionality*

ContractPodAI® provides complete functionality covering the full spectrum of contract management, from creation through to signature and lifecycle management. ContractPodAI® is one of the most comprehensive solutions on the market and will prevent clients from having to procure multiple systems to meet its requirements.

This functionality includes:

- Front door request center to the legal team
- Storage in a highly searchable central repository with optical character recognition (OCR) capability
- Detailed business intelligence reporting and analytics
- Contract creation and assembly
- Access to Leah, the world’s first artificially intelligent contract analyst
- Electronic (E)-signature by DocuSign
- Sophisticated workflows and approval process management
- Robust alerts and reminders for key dates and obligations

*Leah - World’s First Artificially Intelligent Contract Analyst*

ContractPodAI® provides access to Leah, the world’s first artificially intelligent contract analyst. Built on technologies including OpenAI, Zuva AI, International Business Machines (IBM) Watson, and other proprietary AIs - Leah will permanently transform contract creation and automation by reviewing, interpreting and analyzing contracts for key dates and an extensive set of standard key obligations. This information will be automatically populated into the contract record, providing substantial savings in manual data entry as well as the time taken to review contracts.

*Transactions Processing and Reporting*

Transactions are not processed as part of any services provided to clients within the system portal by ContractPodAI®. Clients are able to access information, reports, and initiate transactions available within an end-to-end contract lifecycle management system portal.

ContractPodAI® helps businesses to create automated contracts, build approval workflows and version controls, provides e-signature functionality, tracks - metadata, alerts, reminders, activities and workflows along with user access permissions.

*Significant Events*

ContractPodAI has implemented procedures to capture and address significant events and conditions.

Application alerts include automated e-mail notifications, which are triggered for the following events:

1. Request Generation
2. Contract Generation
3. Important Dates
    a. Expiry Date - Reminder Notification
    b. Renewal Date - Reminder Notification
    c. Custom Date (Max up to 3) - Reminder Notification
4. Changes to Important Dates/Key Obligations Update
5. Activity and Notes
    a. Task Deadline/Activity Reminder
    b. Assignment or Re-assignment of Activity
6. Contract Overdue
7. Approval Workflow
    a. Approval E-mail
    b. Send for Approval (Manual)
8. Signature Completion
    a. Notification from DocuSign
    b. Notification from ContractPodAI
9. Customer Portal
10. Completion of Task

The following notifications and alerts are configured for the infrastructure supporting the ContractPodAI® application:

1. Storage consumption capacity (warning and critical)
2. Compute capacity (storage, central processing unit (CPU) and memory)
3. Database (backup validation, job failure, query processing threshold)
4. File Integrity Monitoring (FIM) (application files)
5. Web application firewall (WAF) (ingress/egress)
6. Virtual Private Network (VPN): Ingress/Egress
7. Server health monitoring: Azure health
8. Application health monitoring with continuum

*Functional Areas of Operation*

The ContractPodAI staff provides support for the above services in each of the following functional areas:

- Executive Management - provides general oversight and strategic planning of operations
- Infra/System Management - responsible for infrastructure and system availability and maintenance
- Development team - responsible for ContractPodAI® product enhancement, new features, bug fixes and overall product support deliveries
- Quality Assurance (QA) Team - verifies that the system complies with the functional specification through functional testing procedures

- Implementation/Transformation Team - responsible for product implementation/configuration and Ai training
- Customer Success Team- responsible for ongoing account management, product updates, and first tier support for product and service issues
- Audit and Compliance - performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements

**Boundaries of the System**

The scope of this report includes the AI Based Contract Management Solutions Services System performed in the Mumbai, India; London, England; Toronto, Canada; New York, New York; San Francisco, California; and Glasgow, Scotland facilities.

**Subservice Organizations**

This report does not include the cloud hosting services provided by Azure at the Ireland, Netherlands, United States, Australia, and Canada facilities.

*Subservice Description of Services*

Azure is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers.

*Complementary Subservice Organization Controls*

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

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

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

| Subservice Organization - Azure | |
|---|---|
| **Control Objective** | **Control** |
| | Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems. |
| | Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses. |
| | Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities. |
| | Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. |
| | Customer data is automatically replicated within Azure to minimize isolated faults. |
| | Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately. |
| Backups | Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities. |
| | Customer data is automatically replicated within Azure to minimize isolated faults. |
| | DPS backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately. |
| | Offsite backups are tracked and managed to maintain accuracy of the inventory information. |

ContractPodAI management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, ContractPodAI performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with the subservice organization
- Reviewing attestation reports over services provided by the subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

### Significant Changes Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization’s last review.

## CONTROL ENVIRONMENT

### Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of ContractPodAI's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of ContractPodAI's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual
- Background checks are performed for employees as a component of the hiring process

### Commitment to Competence

ContractPodAI's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel in certain positions

### Management's Philosophy and Operating Style

ContractPodAI's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole

### Organizational Structure and Assignment of Authority and Responsibility

ContractPodAI's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

ContractPodAI's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

### Human Resources Policies and Practices

ContractPodAI's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensure the service organization operates at maximum efficiency. ContractPodAI's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement upon hire
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

## RISK ASSESSMENT

ContractPodAI's risk assessment process identifies and manages risks that could potentially affect ContractPodAI's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. ContractPodAI identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by ContractPodAI, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

ContractPodAI has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. ContractPodAI attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

## CONTROL OBJECTIVE AND RELATED CONTROL ACTIVITIES

### Integration with Risk Assessment

Along with assessing risks, ContractPodAI has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of those objectives.

### Selection and Development of Control Activities Specified by the Service Organization

Control activities are a part of the process by which ContractPodAI strives to achieve its business objectives. ContractPodAI has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed and improved when necessary to meet the overall objectives of the organization.

ContractPodAI's control objectives and related control activities are included in Section 4 (of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the control objectives and related control activities are included in Section 4, they are, nevertheless, an integral part of ContractPodAI's description of the AI Based Contract Management Solutions Services System.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, adjacent to the service organization's description of control activities. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

## MONITORING

Management monitors controls to ensure that they are operating as intended and that controls are modified as per the change. ContractPodAI's management performs monitoring activities to continuously assess the quality of internal controls over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

### On-Going Monitoring

ContractPodAI defined an internal controls matrix which defines monitoring activities and audit frequency. This review ensures the effectiveness of the control and the monitoring of the process flow on a regular basis.

The control review matrix includes access control, security control, employee and asset management controls, QA, vulnerability assessment and penetration testing, and risk assessment etc. related control reviews. Reports from these reviews are provided to management informing them of any discrepancies in the process or potential risks.

**Reporting Deficiencies**

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

## INFORMATION AND COMMUNICATION SYSTEMS

### Information Systems

ContractPodAI has implemented mechanisms to track and record operational data to make strategic decisions and ensure objectives are consistently achieved. Information gathered from systems enable ContractPodAI to understand business trends in order to maximize efforts and provide optimal services.

*Infrastructure*

Primary infrastructure used to provide ContractPodAI's AI Based Contract Management Solutions Services System includes the following:

| Primary Infrastructure | | |
|---|---|---|
| **Hardware** | **Type** | **Purpose** |
| Servers and Infrastructure | Azure Cloud | Application hosting and processing |
| Firewall | Azure WAF | Ingress/egress monitoring |
| VPN | Azure VPN | Support Team logging into the Infrastructure |
| Server and Application monitoring | Azure Monitor | Server, Services, and Infrastructure monitoring |
| Microsoft Defender | Endpoint Protection and Threat Management System | Endpoint security |
| Structured Query Language (SQL) Server | Windows | Database |
| Microsoft Sentinel | Security Information and Event Management (SIEM) | For monitoring purpose |

*Software*

Primary software used to provide ContractPodAI's AI Based Contract Management Solutions Services System includes the following:

| Primary Software | |
|---|---|
| **Software** | **Purpose** |
| ContractPodAI® | In-scope application for contract management |
| Microsoft Office 365 | Office Productivity |

| Primary Software | |
|---|---|
| **Software** | **Purpose** |
| Visual Studio 2019 | Development Studio |
| DocuSign | E-Signature |
| Azure Cognitive Search | Fluid Search Engine |
| Aspose Portable Documents Format (PDF) | Document Convertor |
| Aspose Word | Document Convertor |
| Aspose for DotNet | Document Convertor |
| MIcrosoft.NET | Development Framework |
| C# | Development Language |
| IBM Watson Ai | Artificial Intelligence |
| Zuva Ai | Artificial Intelligence |
| ABBy Fine Reader | OCR Platform Services |
| Sentry.io | System and Error Logging and View |
| SharePoint | Document Repository |
| Entra ID | Manages users and devices throughout the organization |
| OpenAI | Large Language Model Services |
| Anthropic | Large Language Model Services |

**Communication Systems**

Information and communication is an integral component of ContractPodAI’s internal control system. It is the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage, and control the entity’s operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology (IT). At ContractPodAI, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, meetings are held annually to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate ContractPodAI staff via e-mail messages or from the Company internal Portal.

Specific information systems used to support ContractPodAI’s system are described in the Description of Services section above.

## COMPLEMENTARY USER ENTITY CONTROLS

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

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

*Control Objective 1 - Information Security*

1. User entities are responsible for notifying ContractPodAI of changes made to technical or administrative contact information within their organization.
2. User entities are responsible for maintaining their own system(s) of record outside of the ContractPodAI Application.
3. User entities are responsible for ensuring the supervision, management, and control of the use of ContractPodAI services by their personnel.
4. User entities are responsible for notifying ContractPodAI of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers maintained by the user entity.

*Control Objective 3 - Computer Operations - Availability*

1. User entities are responsible for performing their own business continuity and disaster recovery planning in the event the ContractPodAI application may not be available.

*Control Objective 6 - Client Reporting*

1. User entities are responsible for scheduling their own reports to be delivered timely and to the accurate personnel. These reports may include:
   a. Request and Contract generation
   b. Key Obligation dates
   c. Contract changes
   d. User access
   e. User and Contract activity reports
2. User entities are responsible for monitoring the timely receipt of the reports within the application.
3. User entities are responsible for notifying their Customer Success Manager (CSM) of any reporting errors within the application.

*Control Objective 7 - New Customer Setup and Implementation*

1. User entities are responsible for providing the listing of users and access roles for account setup.
2. User entities are responsible for notifying their CSM of any changes required after the initial account setup.

*Control Objective 8 - Transaction Input*

1. User entities are responsible for inputting complete and accurate information into the ContractPodAI portal.

2. User entities are responsible for making ContractPodAI aware of any issues after go-live implementation.

*Control Objective 9 - Transaction Validation*

1. User entities are responsible for identifying invalid transactions and errors that are entered into the ContractPodAI portal.
2. User entities are responsible for re-entering data into the ContractPodAI portal upon discovery of an invalid transaction or error.

*Control Objective 10 - Transaction Processing*

1. User entities are responsible for ensuring timely processing of data within the ContractPodAI portal.
2. User entities are responsible for transactions being reported in accordance with their specific business rules.
3. User entities are responsible for making ContractPodAI aware of any issues after go-live implementation.

*Control Objective 12 - Vendor Management*

1. ContractPodAI has defined the following activities to oversee controls performed by vendors that could impact the AI Based Contract Management Solutions Services System:
    a. Holding periodic discussions with the subservice organization.
    b. Reviewing attestation reports over services provided by the subservice organization.
    c. Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

# SECTION 4

# DESCRIPTION OF CONTRACTPOD TECHNOLOGIES INC.’S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR’S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

# GUIDANCE REGARDING DESCRIPTION OF CONTRACTPOD TECHNOLOGIES INC.'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

A-LIGN ASSURANCE's examination of the controls of ContractPodAI was limited to the control objectives and related control activities specified by the management of ContractPodAI and did not encompass all aspects of ContractPodAI's operations or operations at user organizations. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18).

Our examination of the control activities was performed using the following testing methods:

| TEST | DESCRIPTION |
|---|---|
| Inquiry | The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information. |
| Observation | The service auditor observed application of the control activities by client personnel. |
| Inspection | The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities. |
| Re-performance | The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control. |

In determining whether a SSAE 18 report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the processing of the user organization's transactions;
- Understand the flow of significant transactions through the service organization;
- Determine whether the control objectives are relevant to the user organization's financial statement assertions;
- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the user organization's financial statements and determine whether they have been implemented.

**CONTROL AREA 1 INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | **General** | | |
| 1.1 | Documented information security policies and procedures are in place to guide personnel in managing system access and protecting information assets and data. | Inspected the information security policies and procedures to determine that documented information security policies and procedures were in place to guide personnel in managing system access and protecting information assets and data. | No exceptions noted. |
| 1.2 | Logical access to systems is approved and granted to an employee as a component of the hiring process. | Inquired of the Senior Security Engineer regarding onboarding procedures to determine that logical access to systems was approved and granted to an employee as a component of the hiring process. | No exceptions noted. |
| | | Inspected the hiring procedures, in-scope user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process. | No exceptions noted. |
| 1.3 | Logical access to systems is revoked as a component of the termination process. | Inquired of the Senior Security Engineer regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process. | No exceptions noted. |
| | | Inspected the termination procedures, in-scope user listings, and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process. | No exceptions noted. |
| 1.4 | Logical access reviews are performed on at least an annual basis. | Inquired of the Senior Security Engineer regarding user access reviews to determine that logical access reviews were performed on at least an annual basis. | No exceptions noted. |
| | | Inspected the completed user access review to determine that logical access reviews were performed on at least an annual basis. | No exceptions noted. |

**CONTROL AREA 1 INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | **Network (Entra ID)** | | |
| 1.5 | Entra ID user access is restricted via role-based security privileges defined within the access control system. | Inquired of the Consultant regarding network access to determine that Entra ID user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | Inspected the Entra ID user listing and access rights to determine that Entra ID user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| 1.6 | Entra ID administrative access is restricted to user accounts accessible by authorized personnel. | Inquired of the Consultant regarding Entra ID administrative access to determine that Entra ID administrative access was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| | | Inspected the Entra ID administrator user listing and access rights to determine that Entra ID administrative access was restricted to user accounts accessible by authorized personnel. | No exceptions noted. |
| 1.7 | Entra ID is configured to enforce password requirements that include:<br>• Password history<br>• Password maximum age<br>• Password length<br>• Complexity<br>• Multi-factor authentication | Inspected the Entra ID password configurations to determine that Entra ID was configured to enforce password requirements that included:<br>• Password history<br>• Password maximum age<br>• Password length<br>• Complexity<br>• Multi-factor authentication | No exceptions noted. |
| 1.8 | Entra ID account lockout settings are in place that include:<br>• Account lockout duration<br>• Account lockout threshold | Inspected the Entra ID account lockout configurations to determine that Entra ID account lockout settings were in place that included:<br>• Account lockout duration<br>• Account lockout threshold | No exceptions noted. |

**CONTROL AREA 1 INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 1.9 | Entra ID audit logging settings are in place that include:<br>• Logon events<br>• System events | Inspected the Entra ID audit logging configurations and an example Entra ID audit log extract to determine that Entra ID audit logging configurations were in place that included:<br>• Logon events<br>• System events | No exceptions noted. |
| 1.10 | Entra ID audit logs are maintained and reviewed as needed. | Inquired of the Consultant regarding Entra ID audit logging to determine that Entra ID audit logs were maintained and reviewed as needed. | No exceptions noted. |
| | | Inspected the Entra ID audit logging configurations and an example Entra ID audit log extract to determine that Entra ID audit logs were maintained and reviewed as needed. | No exceptions noted. |
| | **Production Server (Windows)** | | |
| 1.11 | Production server user access is restricted via role-based security privileges defined within the access control system. | Inquired of the Consultant regarding production server access to determine that production server user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | Inspected the production server user listing and access roles to determine that production server user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| 1.12 | Production server administrative access is restricted to authorized personnel. | Inquired of the Consultant regarding administrative access to determine that production server administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | Inspected the production server administrator user listing and access roles to determine that production servers administrative access was restricted to authorized personnel. | No exceptions noted. |

**CONTROL AREA 1 INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 1.13 | Production servers are configured to use Entra ID for single sign-on (SSO). | Inspected the production server password configurations to determine that production servers were configured to use Entra ID for SSO. | No exceptions noted. |
| | **Production Database (SQL)** | | |
| 1.14 | Production database user access is restricted via role-based security privileges defined within the access control system. | Inquired of the Consultant regarding production database access to determine that production databases user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | Inspected the production database user listing and access roles to determine that production databases user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| 1.15 | Production database administrative access is restricted to authorized personnel. | Inquired of the Consultant regarding administrative access to determine that database administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | Inspected the production database administrator user listing and access roles to determine that production databases administrative access was restricted to authorized personnel. | No exceptions noted. |
| 1.16 | SQL databases are configured to use mixed mode authentication. | Inspected the SQL authentication configurations to determine that SQL databases were configured to use mixed mode authentication. | No exceptions noted. |

**CONTROL AREA 1 INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 1.17 | Production databases are configured to enforce password requirements that include:<br>• Password history<br>• Maximum password age<br>• Password length<br>• Complexity | Inspected the production database password configurations to determine that production databases were configured to enforce password requirements that included:<br>• Password history<br>• Maximum password age<br>• Password length<br>• Complexity | No exceptions noted. |
| 1.18 | Production database authentication relies on AD authentication. | Inspected the production database account lockout configurations to determine that production database authentication relied on AD authentication. | No exceptions noted. |
| 1.19 | Production database audit logging configurations are in place that include failed logon events. | Inspected the production databases audit logging configurations and an example production database audit log extract to determine that production databases audit logging configurations were in place that include failed logon events. | No exceptions noted. |
| 1.20 | Production database audit logs are maintained for review when needed. | Inquired of the Consultant regarding the production databases audit logs to determine that the production databases audit logs were maintained for review when needed. | No exceptions noted. |
| | | Inspected the production database audit logging configurations and an example production database audit log extract to determine that production databases audit logs were maintained for review when needed. | No exceptions noted. |
| | **Application (ContractPodAI®)** | | |
| 1.21 | Production application user access is restricted via role-based security privileges defined within the access control system. | Inquired of the Consultant regarding production application access to determine that production application user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |

**CONTROL AREA 1** **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the production application user listing and access roles to determine that production application user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| 1.22 | Production application administrative access is restricted to authorized personnel. | Inquired of the Consultant regarding administrative access to determine that production application administrative access was restricted to authorized personnel. | No exceptions noted. |
| | | Inspected the production application administrator user listing and access roles to determine that production application administrative access was restricted to authorized personnel. | No exceptions noted. |
| 1.23 | The production application is configured to enforce password requirements that include:<br>• Password history<br>• Maximum password age<br>• Password length<br>• Complexity | Inspected the production application password configurations to determine that applications were configured to enforce password requirements that included:<br>• Password history<br>• Maximum password age<br>• Password length<br>• Complexity | No exceptions noted. |
| 1.24 | Application account lockout settings are in place that include account lockout threshold. | Inspected the application account lockout settings to determine that application account lockout settings were in place that included account lockout threshold. | No exceptions noted. |

**CONTROL AREA 1** **INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 1.25 | Production application audit policy settings are in place that include:<br>• Request ID<br>• User ID<br>• Contract ID<br>• Action Taken | Inspected the production application audit logging configurations and an example production application audit log extract to determine that production application audit logging configurations were in place that included:<br>• Request ID<br>• User ID<br>• Contract ID<br>• Action Taken | No exceptions noted. |
| 1.26 | Production application audit logs are maintained for review when needed. | Inquired of the Consultant regarding application audit logs to determine that application audit logs were maintained for review when needed. | No exceptions noted. |
| | | Inspected the production application audit logging configurations and an example production application audit log extract to determine that production application audit logs were maintained for review when needed. | No exceptions noted. |
| | **Remote Access (Azure VPN)** | | |
| 1.27 | VPN user access is restricted via role-based security privileges defined within the access control system. | Inquired of the Consultant regarding VPN access to determine that VPN user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | Inspected the VPN user listing and access rights to determine that VPN user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| 1.28 | The ability to administer VPN access is restricted to authorized personnel. | Inquired of the Consultant regarding administrative access to the VPN to determine that the ability to administer VPN access was restricted to authorized personnel. | No exceptions noted. |

**CONTROL AREA 1 INFORMATION SECURITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition or deletion.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 1.29 | VPN users are authenticated via MFA prior to being granted remote access to the system. | Inspected the VPN administrator user listing to determine that the ability to administer VPN access was restricted to authorized personnel. | No exceptions noted. |
| | | Observed a user access the in-scope environment remotely to determine that users authenticated via multi-factor authentication prior to being granted remote access to the environment. | No exceptions noted. |
| | | Inspected the VPN authentication configurations to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system. | No exceptions noted. |

## CONTROL AREA 2 DATA COMMUNICATIONS

Control Objective Specified by the Service Organization: Controls activities provide reasonable assurance that data transmissions between the service organization and its clients are complete, accurate, and secure and that data received is posted to the relevant systems in accordance with the Company's guidelines.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 2.1 | Policies and procedures are in place to guide users in the governance of the network security practices. | Inspected the information security policies and procedures to determine that those policies and procedures were in place to guide users in the governance of the network security practices. | No exceptions noted. |
| 2.2 | A firewall is in place to filter unauthorized inbound network traffic from the Internet. | Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet. | No exceptions noted. |
| | | Inspected the firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet. | No exceptions noted. |
| 2.3 | The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. | Inspected the network diagram and the firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule. | No exceptions noted. |
| 2.4 | Network Address Translation (NAT) functionality is utilized to manage internal Internet protocol (IP) addresses. | Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses. | No exceptions noted. |
| 2.5 | Server certificate-based authentication is used as part of the Transport Layer Security (TLS) encryption with a trusted certificate authority. | Inspected the encryption configurations for data in transit and to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority. | No exceptions noted. |
| 2.6 | Users are authenticated via multi-factor authentication prior to being granted remote access to the environment. | Inquired of the Consultant regarding VPN authentication to determine that VPN users authenticated via multi-factor authentication prior to being granted remote access to the system. | No exceptions noted. |
| | | Observed a user access the in-scope environment remotely to determine that users authenticated via multi-factor authentication prior to being granted remote access to the environment. | No exceptions noted. |

**CONTROL AREA 2** **DATA COMMUNICATIONS**

Control Objective Specified by the Service Organization: Controls activities provide reasonable assurance that data transmissions between the service organization and its clients are complete, accurate, and secure and that data received is posted to the relevant systems in accordance with the Company's guidelines.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the VPN authentication configurations to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system. | No exceptions noted. |
| 2.7 | An intrusion prevention system (IPS) is utilized to analyze network events and report possible or actual network security breaches. | Inspected the network diagram and IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches. | No exceptions noted. |
| 2.8 | The IPS is configured to notify personnel upon intrusion prevention. | Inspected the IPS configurations and an example IPS alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention. | No exceptions noted. |

## CONTROL AREA 3 COMPUTER OPERATIONS - AVAILABILITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system processing is authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete accurate and timely manner.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 3.1 | The entity has an incident handling policy in place to provide reasonable assurance that systems are maintained in a manner that helps ensure system availability. | Inspected the incident response policies and procedures to determine that the entity had an incident handling policy in place to provide reasonable assurance that systems were maintained in a manner that helps ensure system availability. | No exceptions noted. |
| 3.2 | Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. | Inquired of the Senior Security Engineer regarding security incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. | No exceptions noted. |
| | | Inspected the incident response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. | No exceptions noted. |
| | | Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. | No exceptions noted. |
| 3.3 | An enterprise monitoring application is utilized to monitor servers and network devices. | Inspected the monitoring system configurations to determine that an enterprise monitoring application was utilized to monitor servers and network devices. | No exceptions noted. |
| 3.4 | The enterprise monitoring application is configured to notify IT personnel when predefined thresholds are exceeded on servers and network devices. | Inspected the monitoring system notification configurations and an example alert to determine that the enterprise monitoring application was configured to notify IT personnel when predefined thresholds were exceeded on servers and network devices. | No exceptions noted. |

## CONTROL AREA 3 COMPUTER OPERATIONS - AVAILABILITY

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system processing is authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete accurate and timely manner.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 3.5 | An IPS is utilized to analyze network events and report possible or actual network security breaches. | Inspected the network diagram and IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches. | No exceptions noted. |
| 3.6 | The IPS is configured to notify personnel upon intrusion prevention. | Inspected the IPS configurations and an example IPS alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention. | No exceptions noted. |
| 3.7 | A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. | Inspected the business continuity and disaster recovery plans to determine that a business continuity and disaster recovery plan was documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations. | No exceptions noted. |
| 3.8 | Business continuity and disaster recovery plans are tested on an annual basis. | Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis. | No exceptions noted. |
| 3.9 | Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. | Inspected the antivirus software dashboard console and the centralized antivirus software configurations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software. | No exceptions noted. |
| 3.10 | The antivirus software is configured to scan workstations on a continuous basis. | Inspected the centralized antivirus software configurations to determine that the antivirus software was configured to scan workstations on a daily basis. | No exceptions noted. |

**CONTROL AREA 3** **COMPUTER OPERATIONS - AVAILABILITY**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that system processing is authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete accurate and timely manner.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 3.11 | The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. | Inspected the centralized antivirus software configurations to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available. | No exceptions noted. |

**CONTROL AREA 4** **COMPUTER OPERATIONS - BACKUP**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that timely system backups of critical files to an off-site location are performed.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 4.1 | Data backup and restore procedures are in place to guide personnel in performing backup activities. | Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities. | No exceptions noted. |
| 4.2 | An automated backup system is utilized to perform scheduled system backups. | Inspected the backup system configurations and backup schedule to determine that an automated backup system was utilized to perform scheduled system backups. | No exceptions noted. |
| 4.3 | Full backups of certain application and database components are performed on a daily basis and transaction log backups are performed on a daily basis. | Inspected the backup schedule, configurations and an example backup history log to determine that full backups of certain application and database components were performed on a daily basis and transaction log backups were performed on a daily basis. | No exceptions noted. |
| 4.4 | When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure. | Inspected the backup configurations and the backup alert for an example failed backup to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure. | No exceptions noted. |
| 4.5 | Backup media is stored in an encrypted format. | Inspected the encryption configurations for backup media to determine that backup media was stored in an encrypted format. | No exceptions noted. |
| 4.6 | The ability to restore backed up data is restricted to authorized personnel. | Inquired of the Consultant regarding restoring backed up data to determine that the ability to restore backups was restricted to authorized personnel. | No exceptions noted. |
| | | Inspected the listing of users with the ability to restore backups to determine that the ability to restore backups was restricted to authorized personnel. | No exceptions noted. |
| 4.7 | Data backed up is replicated to a secondary region in real-time. | Inspected the backup replication configurations to determine that data backed up was replicated to a secondary region in real-time. | No exceptions noted. |

**CONTROL AREA 5** **APPLICATION CHANGE CONTROL**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that new development of and changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 5.1 | Documented change control policies and procedures are in place to guide personnel in the change management process. | Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process. | No exceptions noted. |
| 5.2 | Documented change requests are completed for application changes. | Inspected the supporting change ticket for a sample of system changes to determine that documented change requests were completed for application changed. | No exceptions noted. |
| 5.3 | System change requests are documented and tracked in a ticketing system. | Inspected the supporting change ticket for a sample of system changes to determine that system change requests were documented and tracked in a ticketing system. | No exceptions noted. |
| 5.4 | Version control software is utilized to centrally maintain source code versions and promote application source code through the development process. | Inspected the change control software settings to determine that version control software was utilized to centrally maintain source code versions and promoted application source code through the development process. | No exceptions noted. |
| 5.5 | Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed. | Inspected the change control software configurations to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed. | No exceptions noted. |
| 5.6 | Development and test environments are logically separated from the production environment. | Inquired of the Consultant regarding separate development, test, and production environments to determine that development and test environments were logically separated from the production environment. | No exceptions noted. |
| | | Inspected the separate development, QA and production environments to determine that development and test environments were logically separated from the production environment. | No exceptions noted. |

**CONTROL AREA 5** **APPLICATION CHANGE CONTROL**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that new development of and changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 5.7 | System changes are tested prior to implementation. Types of testing performed depend on the nature of the change. | Inspected the supporting change ticket for a sample of system changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change. | No exceptions noted. |
| 5.8 | System changes are authorized and approved by management prior to implementation. | Inspected the supporting change ticket for a sample of system changes to determine that system changes were authorized and approved by management prior to implementation. | No exceptions noted. |
| 5.9 | The ability to migrate changes into the production environment is restricted to authorized and appropriate users. | Inquired of the Consultant regarding the ability to migrate changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users. | No exceptions noted. |
| | | Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users. | No exceptions noted. |
| 5.10 | FIM software is utilized to help detect unauthorized changes within the production environment. | Inspected the FIM configurations to determine that FIM software was utilized to help detect unauthorized changes within the production environment. | No exceptions noted. |
| 5.11 | The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. | Inspected the FIM software and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected. | No exceptions noted. |

## CONTROL AREA 5 APPLICATION CHANGE CONTROL

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that new development of and changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 5.12 | Developers do not have access to implement changes to the production environment. | Inspected the list of developers and the list of users with access to implement changes to the production environment to determine that developers do have access to implement changes to the production environment. | No exceptions noted. |
| 5.13 | Information security policies and procedures document the baseline requirements for configuration of IT systems and tools. | Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools. | No exceptions noted. |
| 5.14 | Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation. | Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation. | No exceptions noted. |
| 5.15 | System changes are communicated to both affected internal and external users. | Inspected the example e-mail sent to internal users and the example newsletter sent to external users to determine that system changes were communicated to both affected internal and external users. | No exceptions noted. |
| 5.16 | The entity creates test data using data masking software that replaces confidential information with test information during the change management process. | Inspected the data masking software and a set of fictitious data used during development activities to determine that the entity created test data using data masking software that replaced confidential information with test information during the change management process. | No exceptions noted. |
| 5.17 | Changes implemented into the production environment trigger an alert to affected users. | Inspected the change control software configurations and an example alert to determine that changes implemented into the production environment triggered an alert to affected users. | No exceptions noted. |

## CONTROL AREA 6 CLIENT REPORTING

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that client reports are complete and accurate, and reports are made available to clients.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 6.1 | Documented change control policies and procedures are in place to guide personnel in the change management process. | Inspected the IT change management policy to determine that documented change control policies and procedures were in place to guide personnel in the change management process. | No exceptions noted. |
| 6.2 | Report change request are documented and tracked in a ticketing system. | Inquired of the Senior Security Engineer regarding report changes to determine that report change requests were documented and tracked in a ticketing system. | No exceptions noted. |
| | | Inspected the IT change management policy to determine that report change requests were documented and tracked in a ticketing system. | No exceptions noted. |
| | | Inspected the supporting change ticket for a sample of report changes to determine that report change requests were documented and tracked in a ticketing system. | No exceptions noted. |
| 6.3 | User acceptance testing (UAT) is performed on report changes prior to implementation. | Inquired of the Senior Security Engineer regarding UAT performed on report changes to determine that UAT was performed on report changes prior to implementation. | No exceptions noted. |
| | | Inspected the IT change management policy to determine that UAT was performed on report changes prior to implementation. | No exceptions noted. |
| | | Inspected the supporting change ticket for a sample of UAT records to determine that UAT was performed on report changes prior to implementation. | No exceptions noted. |
| 6.4 | Report changes are approved prior to implementation. | Inquired of the Senior Security Engineer regarding approval for report changes prior to deployment to determine that report changes were approved prior to implementation. | No exceptions noted. |

**CONTROL AREA 6 CLIENT REPORTING**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that client reports are complete and accurate, and reports are made available to clients.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 6.5 | Post-implementation testing is performed for report changes to ensure that scheduling functionality works as intended. | Inspected the IT change management policy to determine that report changes were approved prior to implementation. | No exceptions noted. |
| | | Inspected the supporting change ticket for a sample of report changes to determine that report changes were approved prior to implementation. | No exceptions noted. |
| | | Inquired of the Senior Security Engineer regarding post-implementation testing performed on report changes to determine that post-implementation testing was performed for report changes to ensure that scheduling functionality worked as intended. | No exceptions noted. |
| | | Inspected the IT change management policy to determine that post-implementation testing was performed for report changes to ensure that scheduling functionality worked as intended. | No exceptions noted. |
| | | Inspected the supporting change ticket for a sample of report changes to determine that post-implementation testing was performed for report changes to ensure that scheduling functionality worked as intended. | No exceptions noted. |
| 6.6 | Report scheduling input edit check settings are in place to prevent input errors. | Inspected the report scheduling settings and input edit check configurations to determine that report scheduling input edit check settings were in place to prevent input errors. | No exceptions noted. |
| 6.7 | Client reporting errors are identified and resolved in a timely manner. | Inspected the supporting ticket for a sample of reporting errors reported by clients to determine that client reporting errors were identified and resolved in a timely manner. | No exceptions noted. |

**CONTROL AREA 7 NEW CUSTOMER SETUP AND IMPLEMENTATION**

Control Objective Specified by the Service Organization: Controls activities provide reasonable assurance that new customers are established on the system in accordance with the applicable contracts and requirements.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 7.1 | Documented new customer setup and implementation policies and procedures are in place to guide personnel in the new customer setup and implementation process. | Inspected the implementation and customer success policy to determine that documented new customer setup and implementation policies and procedures were in place to guide personnel in the new customer setup and implementation process. | No exceptions noted. |
| 7.2 | Requirements for new customer implementations are documented within the contract, project plan and user intake documentation. | Inquired of the Senior Security Engineer regarding new customer implementations to determine requirements for new customer implementations are documented within the contract, project plan and user intake documentation. | No exceptions noted. |
| | | Inspected the implementation and customer success policy to determine requirements for new customer implementations are documented within the contract, project plan and user intake documentation. | No exceptions noted. |
| | | Inspected the executed contract and project plan for a sample of new customers to determine that requirements for new customers implementations were documented within the contract, project plan and user intake documentation. | No exceptions noted. |
| 7.3 | UAT is performed by ContractPodAI and the client (as desired) using the test case file prior to the new customer setup in production. | Inquired of the Senior Security Engineer regarding UAT for new customer setup to determine that UAT was performed by ContractPodAI and the client (as desired) using the test case file prior to the new customer setup in production. | No exceptions noted. |
| | | Inspected the implementation and customer success policy to determine that UAT was performed by ContractPodAI and the client (as desired) using the test case file prior to the new customer setup in production. | No exceptions noted. |

## CONTROL AREA 7 NEW CUSTOMER SETUP AND IMPLEMENTATION

Control Objective Specified by the Service Organization: Controls activities provide reasonable assurance that new customers are established on the system in accordance with the applicable contracts and requirements.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the supporting UAT testing for a sample of new customer setups to determine that UAT was performed by ContractPodAI and the client (as desired) using the test case file prior to the new customer setup in production. | No exceptions noted. |
| 7.4 | Post-implementation testing is performed on new customer implementations to ensure the ContractPodAI portal is configured in accordance with the requirements within the customer's contact, project, and user intake form. | Inquired of the Senior Security Engineer regarding post-implementation testing for new customers to determine that post-implementation testing was performed on new customer implementations to ensure the ContractPodAI portal was configured in accordance with the requirements within the customer's contact, project, and user intake form. | No exceptions noted. |
| | | Inspected the implementation and customer success policy to determine that post-implementation testing was performed on new customer implementations to ensure the ContractPodAI portal was configured in accordance with the requirements within the customer's contact, project, and user intake form. | No exceptions noted. |
| | | Inspected the supporting implementation testing for a sample of new customer setups to determine that post-implementation testing was performed on new customer implementations to ensure the ContractPodAI portal was configured in accordance with the requirements within the customer's contact, project, and user intake form. | No exceptions noted. |
| 7.5 | Customers are assigned a CSM as part of the implementation process to assist with any issues. | Inquired of the Senior Security Engineer regarding CSM's to determine customers are assigned a CSM as part of the implementation process to assist with any issues. | No exceptions noted. |

**CONTROL AREA 7** **NEW CUSTOMER SETUP AND IMPLEMENTATION**

Control Objective Specified by the Service Organization: Controls activities provide reasonable assurance that new customers are established on the system in accordance with the applicable contracts and requirements.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the implementation and customer success policy to determine customers are assigned a CSM as part of the implementation process to assist with any issues. | No exceptions noted. |
| | | Inspected the introduction e-mail and on-boarding documentation for a sample of new customers to determine that customers were assigned a CSM as part of the implementation process to assist with any issues. | No exceptions noted. |
| 7.6 | CSMs provide training to customers as part of the implementation process. | Inquired of the Senior Security Engineer regarding CSM's to determine CSMs provide training to customers as part of the implementation process. | No exceptions noted. |
| | | Inspected the implementation and customer success policy to determine CSMs provide training to customers as part of the implementation process. | No exceptions noted. |
| | | Inspected the training presentation and the training coordination e-mail for a sample of new customers to determine that CSMs provided training to customers as part of the implementation process. | No exceptions noted. |
| 7.7 | A user guide is distributed to customers as a part of the implementation process. | Inquired of the Senior Security Engineer regarding the user guide distributed to customers to determine that a user guide was distributed to customers as a part of the implementation process. | No exceptions noted. |
| | | Inspected the implementation and customer success policy to determine that a user guide was distributed to customers as a part of the implementation process. | No exceptions noted. |

**CONTROL AREA 7** **NEW CUSTOMER SETUP AND IMPLEMENTATION**

Control Objective Specified by the Service Organization: Controls activities provide reasonable assurance that new customers are established on the system in accordance with the applicable contracts and requirements.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
|  |  | Inspected the user guide for a sample of new customers to determine that a user guide was distributed to customers as a part of the implementation process. | No exceptions noted. |

**CONTROL AREA 8 TRANSACTION INPUT**

Control Objective Specified by the Service Organization: Controls activities provide reasonable assurance that client transactions are initially recorded completely, accurately, and in a timely manner.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 8.1 | Documented processing integrity procedures are in place. | Inspected the data integrity policy to determine that documented processing integrity procedures were in place. | No exceptions noted. |
| 8.2 | Input edit check configurations are in place to help prevent input errors. | Inspected the input edit check configurations to determine that input edit check configurations were in place to help prevent input errors. | No exceptions noted. |
| 8.3 | Transaction input errors are identified and resolved in a timely manner. | Inspected the supporting ticket for a sample of input errors to determine that transaction input errors were identified and resolved in a timely manner. | No exceptions noted. |
| 8.4 | Requirements for new and changed workflow implementations are documented, and the change is approved prior to implementation. | Inquired of the Senior Security Engineer regarding requirements for new and changed workflow implementations to determine that requirements for new and changed workflow implementations were documented, and the change was approved prior to implementation. | No exceptions noted. |
| | | Inspected the supporting change ticket for a sample of workflow implementations to determine that requirements for new and changed workflow implementations were documented, and the change was approved prior to implementation. | No exceptions noted. |
| 8.5 | UAT is performed on new and changed workflow implementations prior to implementation. | Inquired of the Senior Security Engineer regarding UAT for new and changed workflow implementations to determine that UAT was performed on new and changed workflow implementations prior to implementation. | No exceptions noted. |
| | | Inspected the data integrity policy to determine that UAT was performed on new and changed workflow implementations prior to implementation. | No exceptions noted. |

**CONTROL AREA 8** **TRANSACTION INPUT**

Control Objective Specified by the Service Organization: Controls activities provide reasonable assurance that client transactions are initially recorded completely, accurately, and in a timely manner.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 8.6 | A go-live email is sent to clients for new and changed workflow implementations. | Inspected the supporting change tickets for a sample of workflow implementations to determine that UAT was performed on new and changed workflow implementations prior to implementation. | No exceptions noted. |
| | | Inquired of the Senior Security Engineer regarding new and changed workflow implementations to determine that a go-live email was sent to clients for new and changed workflow implementations. | No exceptions noted. |
| | | Inspected the implementation and customer success policy to determine that a go-live email was sent to clients for new and changed workflow implementations. | No exceptions noted. |
| | | Inspected the go-live emails for a sample of workflow implementations to determine that a go-live email was sent to clients for new and changed workflow implementations. | No exceptions noted. |

## CONTROL AREA 9 TRANSACTION VALIDATION

Control Objective Specified by the Service Organization: Controls activities provide reasonable assurance that invalid transactions and errors are identified, rejected, and correctly re-entered into the system in a timely manner.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 9.1 | Documented processing integrity procedures are in place. | Inspected the data integrity policy to determine that documented processing integrity procedures were in place. | No exceptions noted. |
| 9.2 | Input edit check configurations are in place to help prevent input errors. | Inspected the input edit check configurations to determine that input edit check configurations were in place to help prevent input errors. | No exceptions noted. |
| 9.3 | Transaction input errors are identified and resolved in a timely manner. | Inspected the supporting ticket for the population of input errors to determine that transaction input errors were identified and resolved in a timely manner. | No exceptions noted. |
| 9.4 | Requirements for new and changed workflow implementations are documented, and the change is approved prior to implementation. | Inquired of the Senior Security Engineer regarding requirements for new and changed workflow implementations to determine that requirements for new and changed workflow implementations were documented, and the change was approved prior to implementation. | No exceptions noted. |
| | | Inspected the supporting change ticket for a sample of workflow implementations to determine that requirements for new and changed workflow implementations were documented, and the change was approved prior to implementation. | No exceptions noted. |
| 9.5 | UAT is performed on new and changed workflow implementations prior to implementation. | Inquired of the Senior Security Engineer regarding UAT for new and changed workflow implementations to determine that UAT was performed on new and changed workflow implementations prior to implementation. | No exceptions noted. |
| | | Inspected the data integrity policy to determine that UAT was performed on new and changed workflow implementations prior to implementation. | No exceptions noted. |

**CONTROL AREA 9 TRANSACTION VALIDATION**

Control Objective Specified by the Service Organization: Controls activities provide reasonable assurance that invalid transactions and errors are identified, rejected, and correctly re-entered into the system in a timely manner.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 9.6 | Post-implementation testing is performed on new and changed workflow implementations to ensure they are working as intended. | Inspected the supporting change tickets for a sample of workflow implementations to determine that UAT was performed on new and changed workflow implementations prior to implementation. | No exceptions noted. |
| | | Inquired of the Senior Security Engineer regarding post-implementation testing for new and changed workflow implementations to determine that post-implementation testing was performed on new and changed workflow implementations to ensure they were working as intended. | No exceptions noted. |
| | | Inspected the implementation and customer success policy to determine post-implementation testing is performed on new and changed workflow implementations to ensure they are working as intended. | No exceptions noted. |
| | | Inspected the go-live emails for a sample of workflow implementations to determine that post-implementation testing was performed on new and changed workflow implementations to ensure they were working as intended. | No exceptions noted. |

**CONTROL AREA 10 TRANSACTION PROCESSING**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that client transactions are processed in a timely manner and reported in accordance with client specific business rules.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 10.1 | Documented processing integrity procedures are in place. | Inspected the data integrity policy to determine that documented processing integrity procedures were in place. | No exceptions noted. |
| 10.2 | Requirements for new and changed workflow implementations are documented, and the change is approved prior to implementation. | Inquired of the Senior Security Engineer regarding requirements for new and changed workflow implementations to determine that requirements for new and changed workflow implementations were documented, and the change was approved prior to implementation. | No exceptions noted. |
| | | Inspected the supporting change ticket for a sample of workflow implementations to determine that requirements for new and changed workflow implementations were documented, and the change was approved prior to implementation. | No exceptions noted. |
| 10.3 | UAT is performed on new and changed workflow implementations prior to implementation. | Inquired of the Senior Security Engineer regarding UAT for new and changed workflow implementations to determine that UAT was performed on new and changed workflow implementations prior to implementation. | No exceptions noted. |
| | | Inspected the data integrity policy to determine that UAT was performed on new and changed workflow implementations prior to implementation. | No exceptions noted. |
| | | Inspected the supporting change tickets for a sample of workflow implementations to determine that UAT was performed on new and changed workflow implementations prior to implementation. | No exceptions noted. |
| 10.4 | A go-live email is sent to clients for new and changed workflow implementations. | Inquired of the Senior Security Engineer regarding new and changed workflow implementations to determine that a go-live email was sent to clients for new and changed workflow implementations. | No exceptions noted. |

**CONTROL AREA 10 TRANSACTION PROCESSING**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that client transactions are processed in a timely manner and reported in accordance with client specific business rules.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the implementation and customer success policy to determine that a go-live email was sent to clients for new and changed workflow implementations. | No exceptions noted. |
| | | Inspected the go-live emails for a sample of workflow implementations to determine that a go-live email was sent to clients for new and changed workflow implementations. | No exceptions noted. |

**CONTROL AREA 11** **CHANGE MANAGEMENT**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that changes to systems are initiated as needed, are authorized and function in accordance with specifications to result in valid, complete, accurate and timely processing and reporting of customer developed functions, collaboration and communication, and protect data from unauthorized changes. and support Segregation of duties exist within the change management process.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 11.1 | Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation. | Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation. | No exceptions noted. |
| 11.2 | Documented change requests are completed for system changes. | Inspected the supporting change ticket for a sample of system changes to determine that documented change requests were completed for system changes. | No exceptions noted. |
| 11.3 | System change requests are documented and tracked in a ticketing system. | Inspected the supporting change ticket for a sample of system changes to determine that system change requests were documented and tracked in a ticketing system. | No exceptions noted. |
| 11.4 | Version control software is utilized to centrally maintain source code versions and promote application source code through the development process. | Inspected the change control software settings to determine that version control software was utilized to centrally maintain source code versions and promoted application source code through the development process. | No exceptions noted. |
| 11.5 | Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed. | Inspected the change control software configurations to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed. | No exceptions noted. |
| 11.6 | Development and test environments are logically separated from the production environment. | Inquired of the Consultant regarding separate development, test, and production environments to determine that development and test environments were logically separated from the production environment. | No exceptions noted. |

**CONTROL AREA 11** **CHANGE MANAGEMENT**

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that changes to systems are initiated as needed, are authorized and function in accordance with specifications to result in valid, complete, accurate and timely processing and reporting of customer developed functions, collaboration and communication, and protect data from unauthorized changes. and support Segregation of duties exist within the change management process.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the separate development, QA and production environments to determine that development and test environments were logically separated from the production environment. | No exceptions noted. |
| 11.7 | System changes are tested prior to implementation. Types of testing performed depend on the nature of the change. | Inspected the supporting change ticket for a sample of system changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change. | No exceptions noted. |
| 11.8 | System changes are authorized and approved by management prior to implementation. | Inspected the supporting change ticket for a sample of system changes to determine that system changes were authorized and approved by management prior to implementation. | No exceptions noted. |
| 11.9 | The ability to migrate changes into the production environment is restricted to authorized and appropriate users. | Inquired of the Consultant regarding the ability to migrate changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users. | No exceptions noted. |
| | | Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users. | No exceptions noted. |
| 11.10 | FIM software is utilized to help detect unauthorized changes within the production environment. | Inspected the FIM configurations to determine that FIM software was utilized to help detect unauthorized changes within the production environment. | No exceptions noted. |

**CONTROL AREA 11** **CHANGE MANAGEMENT**

Control Objective Specified by the Service Organization:

Control activities provide reasonable assurance that changes to systems are initiated as needed, are authorized and function in accordance with specifications to result in valid, complete, accurate and timely processing and reporting of customer developed functions, collaboration and communication, and protect data from unauthorized changes. and support Segregation of duties exist within the change management process.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 11.11 | The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. | Inspected the FIM software and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected. | No exceptions noted. |
| 11.12 | Developers do not have access to implement changes to the production environment. | Inspected the list of developers and the list of users with access to implement changes to the production environment to determine that developers do have access to implement changes to the production environment. | No exceptions noted. |
| 11.13 | Information security policies and procedures document the baseline requirements for configuration of IT systems and tools. | Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools. | No exceptions noted. |
| 11.14 | System changes are communicated to both affected internal and external users. | Inspected the example e-mail sent to internal users and the example newsletter sent to external users to determine that system changes were communicated to both affected internal and external users. | No exceptions noted. |
| 11.15 | The entity creates test data using data masking software that replaces confidential information with test information during the change management process. | Inspected the data masking software and a set of fictitious data used during development activities to determine that the entity created test data using data masking software that replaced confidential information with test information during the change management process. | No exceptions noted. |
| 11.16 | Changes implemented into the production environment trigger an alert to the development team. | Inspected the change control software configurations and an example alert to determine that changes implemented into the production environment triggered an alert to the development team. | No exceptions noted. |

## CONTROL AREA 12 VENDOR MANAGEMENT

Control Objective Specified by the Service Organization: Controls activities provide reasonable assurance that policies and procedures are in place to govern vendor management practices of the organization.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 12.1 | Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances. | Inspected the vendor risk assessment policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances. | No exceptions noted. |
| 12.2 | Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process. | Inspected the vendor management policies and procedures to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process. | No exceptions noted. |
| | | Inspected the completed vendor risk assessment for a sample of third parties to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process. | No exceptions noted. |
| 12.3 | Identified third-party risks are evaluated by management. | Inspected the vendor management policies and procedures to determine that identified third-party risks were evaluated by management. | No exceptions noted. |
| | | Inspected the completed vendor risk assessment for a sample of third parties to determine that identified third-party risks were evaluated by management. | No exceptions noted. |
| 12.4 | The entity's third-party agreement outlines and communicates:<br>• The scope of services<br>• Roles and responsibilities<br>• Terms of the business relationship<br>• Communication protocols<br>• Compliance requirements<br>• Service levels | Inspected the master third-party agreement template to determine that the entity's third-party agreement outlined and communicated:<br>• The scope of services<br>• Roles and responsibilities<br>• Terms of the business relationship<br>• Communication protocols<br>• Compliance requirements<br>• Service levels | No exceptions noted. |

**CONTROL AREA 12 VENDOR MANAGEMENT**

Control Objective Specified by the Service Organization: Controls activities provide reasonable assurance that policies and procedures are in place to govern vendor management practices of the organization.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | Inspected the executed third-party agreement for a sample of third parties to determine that the entity's third-party agreement outlined and communicated:<br>• The scope of services<br>• Roles and responsibilities<br>• Terms of the business relationship<br>• Communication protocols<br>• Compliance requirements<br>• Service levels | No exceptions noted. |
| 12.5 | Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment. | Inspected the completed third-party attestation report and vendor checklist for a sample of third parties that the entity has a relationship with to determine that management obtained and reviewed the attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendors environment. | No exceptions noted. |
| 12.6 | A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements. | Inspected the vendor management policies and procedures to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements. | No exceptions noted. |
| | | Inspected the completed vendor risk assessment for a sample of third parties to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements. | No exceptions noted. |
| 12.7 | Management has established exception handling procedures for services provided by third parties. | Inspected the vendor management policies and procedures to determine that management established exception handling procedures for services provided by third parties. | No exceptions noted. |

**CONTROL AREA 12 VENDOR MANAGEMENT**

Control Objective Specified by the Service Organization: Controls activities provide reasonable assurance that policies and procedures are in place to govern vendor management practices of the organization.

| Control Point | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 12.8 | The entity has documented procedures for addressing issues identified with third parties. | Inspected the vendor management policies and procedures to determine that the entity documented procedures for addressing issues identified with third parties. | No exceptions noted. |
| 12.9 | The entity's third-party agreement outlines and communicates confidentiality commitments and requirements. | Inspected the master third-party agreement template to determine that the entity's third-party agreement outlined and communicated confidentiality commitments and requirements. | No exceptions noted. |
| | | Inspected the executed third-party agreement for a sample of third parties to determine that the entity's third-party agreement outlined and communicated confidentiality commitments and requirements. | No exceptions noted. |
| 12.10 | Management assesses the compliance of confidentiality commitments and requirements of third parties at least annually. | Inspected the completed vendor risk assessment for a sample of third parties to determine that management assessed the compliance of privacy commitments and requirements of third parties at least annually. | No exceptions noted. |