A-LIGN

ContractPod Technologies Ltd

Type 2 SOC 2

2023

ContractPodAi

REPORT ON CONTRACTPOD TECHNOLOGIES LTD'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

Pursuant to Reporting on System and Organization Controls 2 (SOC 2)
Type 2 examination performed under AT-C 105 and AT-C 205

Throughout the Period October 1, 2022 to September 30, 2023

Table of Contents

SECTION 1

ASSERTION OF CONTRACTPOD TECHNOLOGIES LTD MANAGEMENT

ASSERTION OF CONTRACTPOD TECHNOLOGIES LTD MANAGEMENT

November 7, 2023

We have prepared the accompanying description of ContractPod Technologies Ltd's ('ContractPodAi' or 'the Company') ContractPod AI Based Contract Management Solutions Services System titled "ContractPod Technologies Ltd's Description of Its ContractPod AI Based Contract Management Solutions Services System throughout the period October 1, 2022 to September 30, 2023" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the ContractPod AI Based Contract Management Solutions Services System that may be useful when assessing the risks arising from interactions with ContractPodAi's system, particularly information about system controls that ContractPodAi has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

ContractPodAi uses Microsoft Azure ('Azure' or 'subservice organization') to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ContractPodAi, to achieve ContractPodAi's service commitments and system requirements based on the applicable trust services criteria. The description presents ContractPodAi's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ContractPodAi's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at ContractPodAi, to achieve ContractPodAi's service commitments and system requirements based on the applicable trust services criteria. The description presents ContractPodAi's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ContractPodAi's controls.

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

a. the description presents ContractPodAi's ContractPod AI Based Contract Management Solutions Services System that was designed and implemented throughout the period October 1, 2022 to September 30, 2023, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that ContractPodAi's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of ContractPodAi's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that ContractPodAi's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of ContractPodAi's controls operated effectively throughout that period.

Anurag Malik

Anurag Malik
Chief Technology Officer
ContractPod Technologies Ltd

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: ContractPod Technologies Ltd

Scope

We have examined ContractPodAi's accompanying description of its ContractPod AI Based Contract Management Solutions Services System titled "ContractPod Technologies Ltd's Description of Its ContractPod AI Based Contract Management Solutions Services System throughout the period October 1, 2022 to September 30, 2023" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that ContractPodAi's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

ContractPodAi uses Azure to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ContractPodAi, to achieve ContractPodAi's service commitments and system requirements based on the applicable trust services criteria. The description presents ContractPodAi's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ContractPodAi's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at ContractPodAi, to achieve ContractPodAi's service commitments and system requirements based on the applicable trust services criteria. The description presents ContractPodAi's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ContractPodAi's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

ContractPodAi is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that ContractPodAi's service commitments and system requirements were achieved. ContractPodAi has provided the accompanying assertion titled "Assertion of ContractPod Technologies Ltd Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. ContractPodAi is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

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 report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects,

a. the description presents ContractPodAi's ContractPod AI Based Contract Management Solutions Services System that was designed and implemented throughout the period October 1, 2022 to September 30, 2023, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that ContractPodAi's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of ContractPod AI's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that ContractPodAi's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of ContractPodAi's controls operated effectively throughout that period.

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 ContractPod AI Based Contract Management Solutions Services System during some or all of the period October 1, 2022 to September 30, 2023, business partners of ContractPodAi subject to risks arising from interactions with the ContractPod AI Based Contract Management Solutions Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

A-LIGN ASSURANCE

Tampa, Florida
November 7, 2023

SECTION 3

CONTRACTPOD TECHNOLOGIES LTD'S DESCRIPTION OF ITS CONTRACTPOD AI BASED CONTRACT MANAGEMENT SOLUTIONS SERVICES SYSTEM THROUGHOUT THE PERIOD OCTOBER 1, 2022 TO SEPTEMBER 30, 2023

OVERVIEW OF OPERATIONS

Company Background

ContractPodAi was founded in 2012 with the mission to make the end-to-end contract management system more accessible to corporate in-house legal teams and with the aim of eliminating data entry and paralegal related work for the corporate department.

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. It features repository, contract generation, and third-party review functionality. Since going live in 2015, the platform has been helping legal departments at large-scale corporations across the globe digitally transform their contract management function.

Description of Services Provided

ContractPodAi provides complete functionality covering the full spectrum of contract management, from creation through to signature and lifecycle management.

This functionality includes:

- Front door requests to the legal team
- Storage in a highly searchable central repository with Optical Character Recognition (OCR) capability
- Detailed reporting and analytics
- Contract creation and assembly
- Access to Leah, an artificially intelligent contract analyst
- Electronic (E)-signature by DocuSign
- Automated workflows and approval process management
- Robust alerts and reminders for key dates and tracking obligations

ContractPodAi provides access to Leah, an 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 is automatically populated into the contract record, providing substantial savings in manual data entry, as well as the time taken to review contracts.

Principal Service Commitments and System Requirements

ContractPodAi designs its processes and procedures related to its AI Based Contract Management Solutions System to meet its objectives for its contract management services. Those objectives are based on the service commitments that ContractPodAi makes to user entities, the laws and regulations that govern the provision of contract management services, and the operational and compliance requirements that ContractPodAi has established for the services. The contract management services of ContractPodAi are subject to regulations, as well as privacy and security laws and regulations in the jurisdictions in which ContractPodAi operates.

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

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

ContractPodAi establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in ContractPodAi's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the AI Based Contract Management Solutions System.

Components of the System

Infrastructure

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

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Servers and Infrastructure	Azure	Application hosting and processing
Intrusion Prevention System (IPS)	Azure Intrusion Prevention Threat Scanning	Screens and alerts on network traffic based on "malicious Internet Protocol (IP) addresses and domains" as assessed by feeds from the Microsoft Threat Intelligence service
Firewalls	Windows Firewall Advanced Security	Filters inbound and outbound traffic out of the network
Security Information and Event management (SIEM)	Microsoft Sentinel	For monitoring purposes
Virtual Private Network (VPN)	Azure VPN	VPN services
Structured Query Language (SQL) Server	Windows	Database

Software

Primary software used to provide ContractPodAi's ContractPod 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
Visual Studio 2019	Development Studio
DocuSign	E-Signature
Azure Cognitive Search	Fluid Search Engine
Aspose Portable Document Format (PDF)	Document Convertor
Aspose Word	Document Convertor
Aspose for DotNet	Document Convertor
Microsoft.NET	Development Framework
C#	Development Language
IBM Watson AI	AI
Zuva AI	AI
ABBy Fine Reader	OCR Platform Services
Sentry.io	System and Error Logging and View
SharePoint	Document Repository
Active Directory (AD)	Manages users and devices throughout the organization
Azure Storage Service Encryption (SSE)	Encryption-at-rest tool

People

ContractPodAi is organized in the following functional areas:

Senior management staff have overall functional responsibility for commercial, technical, and operational aspects of the business globally. The technical arm is managed out of the Mumbai office.

Finance and Human Resources (HR)/Admin are responsible for the accounts, accounts payable and receivable, and management accounting on a global basis. The team of HR professionals are in three offices, performing HR management, talent acquisition, and payroll/admin functions.

Technology and Development Operations are based largely out of the Mumbai office and involved in platform enhancement, customization, and bug support.

Marketing runs as a global function from the Toronto office and is focused primarily on communications, content, demand, and events.

Sales is globally managed from the New York City and London offices. Both teams consist of leadership, account executives, sales development representatives, and sales engineers.

Transformation is based largely out of London and services the globe. The team consists of implementation managers that run customer implementations from end to end, liaising with the Technology team in Mumbai where necessary. Their entry point on each client project takes place via a handover from the Sales Engineer, at which point the agreement is defined before the point of contract signature. They then own and run the agreement, which defines each client's configuration of the software, and are responsible for client delivery and onboarding.

The Transformation team also features a team of legal engineers, who test and refine the AI review capabilities of the software, feeding back to Technology as appropriate and liaising on the client side to optimize and improve machine learning efficiency on an ongoing basis.

The Customer Success team is based in the New York City office and is a global function. The team takes over each customer just after go-live via a handover from the implementation manager. It is their responsibility to act as a single point of contact for the customer on their user journey with the software, with a responsibility to retain and renew the license as appropriate.

Data

- Transaction data: comes from the creation of contracts in the system. This includes metadata of the contracts and the contract file
- Output reports: Reports that are generated from the system for/by the end users of the system
- Audit Trails: Generated by the Contract Lifecycle Management (CLM) solution for user and system actions
- System files/Code Files: Published code files for the ContractPodAi Software as a Service (SaaS) solutions
- Error logs: Generated by ContractPodAi SaaS product and Windows OS and infrastructure

Processes, Policies and Procedures

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

Physical Security

The in-scope system and supporting infrastructure is hosted by Azure. As such, Azure is responsible for the physical security controls for the in-scope system. For a listing of controls implemented by Azure, please refer to the "Subservice Organizations" section, below.

Logical Access

ContractPodAi uses role-based security, and it requires users to be identified and authenticated prior to any system resources. The application protects its users with its native identity management system.

SharePoint and OneDrive are used as document repositories and rely on authentication from AD user credentials. Both services are hosted on Microsoft Office365.

Employees and approved vendor personnel sign on to the ContractPodAi network using an AD user identification (ID) and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of AD. Passwords conform to defined password standards and are enforced through parameter settings in AD. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Customer employees access ContractPodAi's AI-Based Contract Management Solutions Services system through the Internet using the SSL functionality of their web browser. These customer employees supply a valid user ID and password to gain access to customer cloud resources. Passwords conform to password configuration requirements configured on the Application or system.

Upon hire, employees are assigned to a position in the HR management system. Prior to the employee's start date, HR raises the request to the IT Helpdesk system for assets allocation and access to be granted. This request is then used by the IT Administrator team to allocate the assets and access to specific tools and services as per their role. Access to the tools and services are defined by the employee's line manager and then, as per the tools and services, the request traverses through respective assets/Service owners to provide access. The system lists also include employees with position changes and the associated roles to be changed within the access.

On an annual basis, access requests for each role are reviewed by a working group composed of security help desk, Infrastructure admin team, customer service, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access.

HR personnel create the request in the IT Helpdesk system for the terminated employee on the day of termination. The system then notifies the respective access administrators to revoke the respective access and assigned assets collection.

On an annual basis, HR runs a list of active employees and sends the request to the IT and other system/services owners who manage the access to the other systems and services. The respective access owners check and reconcile the active employee list and remove/revoke access to any tool and service. Any discrepancy in the access is logged into the system and remediation or action is logged.

Computer Operations - Backups

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

Customer's data is hosted within their designated region on Azure in a northern European, United States, and Asia-Pacific (APAC) datacenter along with a continuous replication within the same continental region at a western European, United States, and APAC datacenter. Daily and hourly backups are retained for 90 days within their respective continental region.

The backups of the systems are stored on Azure for quick access when required.

On the workstations side, employees are advised to store data to their respective OneDrive accounts.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to IT incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

ContractPodAi' s dedicated Infrastructure team monitors capacity for both internal and customer instances to ensure uninterrupted service.

The Infrastructure team ensures adherence to a rigorous patch management program within ContractPodAi. Security patches are applied to the systems after rigorous testing.

Business continuity and disaster recovery plans are developed, updated, and tested annually. Additionally, backup restoration tests are also performed annually.

Change Control

ContractPodAi maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, code review, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Customer Success or Implementation Managers approve changes prior to migration to the production environment and document those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate build code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

ContractPodAi has implemented a patch management process to ensure ContractPodAi customer and infrastructure systems are patched in accordance with vendor-recommended operating system patches. ContractPodAi system owners review proposed operating system patches to determine whether the patches are applied. ContractPodAi are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. ContractPodAi staff validate that patches have been installed and, if applicable, that reboots have been completed.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees, controlled by AD.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant system is configured to take its place.

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

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

Authorized employees may access the system using VPN technology. Employees are authenticated through multi-factor authentication (MFA) system via AD.

Boundaries of the System

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

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

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

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 to 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 competency 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 competency levels for particular jobs and has 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 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 Resource 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 HR 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.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process.

Risk Assessment Process

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.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of ContractPodAi's AI Based Contract Management Solutions System; as well as the nature of the components of the system result in risks that the criteria will not be met. ContractPodAi addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, ContractPodAi's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications 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 time frame 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, 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, annual meetings are held 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 personnel via email messages.

Specific information systems used to support ContractPodAi's AI Based Contract Management Solutions System are described in the "Description of Services Provided" section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. ContractPodAi's management performs monitoring activities to continuously assess the quality of internal control 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's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

ContractPodAi has an internal controls matrix for defining different monitoring and audit frequencies. The internal controls matrix ensures the effectiveness of the controls and monitoring of the process flow on a regular basis. The internal controls matrix includes access, security, employee and asset management, quality assurance, and risk assessment related control reviews. A report on these controls is provided to management to inform them of any kind of discrepancy in the processes or potential risk.

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. Corrective actions, if necessary, are documented and tracked within the internal tracking tool.

Changes to the System Since the Last Review

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

Incidents Since the Last Review

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

Criteria Not Applicable to the System

Common/Security, Availability, and Confidentiality criteria were applicable to the ContractPod AI Based Contract Management Solutions Services System.

Subservice Organizations

This report does not include the data center hosting services provided by Azure at multiple 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 the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to ContractPodAi's services to be solely achieved by ContractPodAi control procedures. Accordingly, the subservice organization, 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 trust services criteria described within this report are met:

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4, CC7.2	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		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 data center facility is monitored 24x7 by security personnel.
Availability	A1.2	Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		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.
		Backup restoration procedures are defined, and backup data integrity checks are performed through standard restoration activities.
		Offsite backups are tracked and managed to maintain accuracy of the inventory information.
		Production data is encrypted on backup media.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.

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

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

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

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security, Availability, and Confidentiality Categories)
Security refers to the protection of: i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Control Activities Specified by the Service Organization

The applicable trust services criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of ContractPodAi's description of the system. Any applicable trust services criteria that are not addressed by control activities at ContractPodAi are described within Section 4 and within the "Subservice Organizations" section above.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4. 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.

SECTION 4

TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

A-LIGN ASSURANCE's examination of the controls of ContractPodAi was limited to the Trust Services Criteria, related criteria and control activities specified by the management of ContractPodAi and did not encompass all aspects of ContractPodAi's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

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 the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization
- Determine whether the criteria are relevant to the user entity's assertions
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through the employee handbook.	Inspected the employee handbook on the entity's SharePoint site to determine that core values were communicated from executive management to personnel through the employee handbook.	No exceptions noted.
		An employee handbook is documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook was documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Upon hire, personnel are required to complete a background check.	Inspected the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
		Upon changes, personnel are required to acknowledge the employee handbook and code of conduct.	Inquired of the Director of Information Security regarding the acknowledgment of the employee handbook to determine that upon changes, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the employee handbook to determine that upon changes, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the employee handbook acknowledgement for a sample of current employees to determine that upon changes, personnel were required to acknowledge the employee handbook and code of conduct	Testing of the control activity disclosed that no changes to the employee handbook occurred during the review period.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inquired of the Director of Information Security regarding performance evaluations to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
			Inspected the employee evaluation policies and procedures within the employee handbook to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		.	Inspected the completed performance evaluation for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the employee handbook to determine that sanction policies, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the anonymous reporting form on the company's website to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities are documented and reviewed annually.	Inspected the job description including revision history for a sample of executive management job roles to determine that executive management roles and responsibilities were documented and reviewed annually.	No exceptions noted.
		Executive management defines and documents the skills and expertise needed among its members.	Inspected the job description for a sample of executive management job roles to determine that executive management defined and documented the skills and expertise needed among its members.	No exceptions noted.
		Executive management maintains independence from those that operate the key controls implemented within the environment.	Inspected the organizational chart and the completed internal controls matrix to determine that executive management maintained independence from those that operate the key controls within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management meets quarterly with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the executive management meeting minutes for a sample of quarters to determine that executive management met quarterly with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.
		Executive management evaluates the skills and competencies of those that operate the internal controls within the environment annually.	Inspected the completed performance evaluation for a sample of current employees to determine that executive management evaluated the skills and competencies of those that operate the internal controls within the environment annually.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment on an annual basis.	Inspected the completed internal controls matrix and the executive management meeting minutes to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls implemented within the environment on an annual basis.	No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary.	Inspected the revision history of the organizational chart to determine that executive management reviewed the organization chart annually and made updates to the organizational structure and lines of reporting, if necessary.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the job description including revision history for a sample of roles to determine that executive management reviewed job descriptions annually and made updates, if necessary.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook,.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management has established proper segregations of duties for key job functions and roles within the organization.	Inspected the organizational chart, the completed internal controls matrix, and the job description for a sample of job roles to determine that executive management had established proper segregations of duties for key job functions and roles within the organization.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the vendor management policy and the completed vendor risk assessment for a sample of vendors to determine that a vendor risk assessment was performed on an annual basis, which included reviewing the activities performed by third-parties.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the performance evaluation policy and the training policy to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		The entity evaluates the competencies and experience of candidates prior to hiring.	Inspected the candidate evaluation form for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process.	Inspected the job description and candidate evaluation form for a sample of new hires to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring process.	No exceptions noted.
		The entity works with an outside vendor to attract individuals with competencies and experience that align with the entity's goals and objectives.	Inspected the job postings and the contract for the outside vendor to determine that the entity worked with an outside vendor to attract individuals with competencies and experience that aligned with the entity's goals and objectives.	No exceptions noted.
		Executive management has created a training program for its employees.	Inspected the security training program to determine that executive management had created a training program for its employees.	No exceptions noted.
		Upon hire, employees are required to complete information security and awareness training.	Inspected the security awareness training completion for a sample of new hires to determine that upon hire, employees were required to complete information security and awareness training.	No exceptions noted.
		Current employees are required to complete information security and awareness training on an annual basis.	Inspected the security awareness training completion for a sample of current employees to determine that current employees were required to complete information security and awareness training on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management tracks and monitors compliance with continued professional education training requirements.	Inspected the Continued Professional Education (CPE) training tracker to determine that executive management tracked and monitored compliance with continued professional development training requirements.	No exceptions noted.
		Upon hire, personnel are required to complete a background check.	Inspected the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon changes, personnel are required to acknowledge the employee handbook and code of conduct.	Inquired of the Director of Information Security regarding the acknowledgment of the employee handbook to determine that upon changes, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the employee handbook to determine that upon changes, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the employee handbook acknowledgement for a sample of current employees to determine that upon changes, personnel were required to acknowledge the employee handbook and code of conduct	Testing of the control activity disclosed that no changes to the employee handbook occurred during the review period.
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the performance evaluation policy and the training policy to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inquired of the Director of Information Security regarding performance evaluations to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the employee evaluation policies and procedures within the employee handbook to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
			Inspected the completed performance evaluation for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the job description including revision history for a sample of job roles to determine that executive management reviewed job descriptions annually and made updates, if necessary.	No exceptions noted.
		Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the employee handbook to determine that sanction policies, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Information security policies and procedures are documented and made available to employees through the entity's SharePoint site.	Inspected the information security policy on the entity's SharePoint site to determine that the information security policies and procedures were documented and made available to employees through the entity's SharePoint site.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inquired of the Director of Information Security regarding the edit check configurations to determine that edits checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
			Inspected the edit check error configurations to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
		A data flow diagram is documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the data flow diagram to determine that a data flow diagram was documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data that entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the file integrity monitoring (FIM) configurations, IPS configurations, and encryption configurations for data in transit and data at rest to determine that data that entered into the system, processed by the system, and output from the system was protected from unauthorized access.	No exceptions noted.
		Data is only retained for as long as required to perform the required system functionality, service or use.	Inspected the information security policy to determine that data was only retained for as long as required to perform the required system functionality, service or use.	No exceptions noted.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		The entity's policies and procedures and employee handbook are made available to employees through the entity's SharePoint site.	Inspected the employee handbook and the information security policy on the entity's SharePoint site to determine that the entity's policies and procedures and employee handbook were made available to employees through the entity's SharePoint site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, employees are required to complete information security and awareness training.	Inspected the security awareness training completion for a sample of new hires to determine that upon hire, employees were required to complete information security and awareness training.	No exceptions noted.
		Current employees are required to complete information security and awareness training on an annual basis.	Inspected the security awareness training completion for a sample of current employees to determine that current employees were required to complete information security and awareness training on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Upon changes, personnel are required to acknowledge the employee handbook and code of conduct.	Inquired of the Director of Information Security regarding the acknowledgment of the employee handbook to determine that upon changes, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the employee handbook to determine that upon changes, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the employee handbook acknowledgement for a sample of current employees to determine that upon changes, personnel were required to acknowledge the employee handbook and code of conduct	Testing of the control activity disclosed that no changes to the employee handbook occurred during the review period.
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the executive management meeting minutes to determine that executive management met annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the anonymous reporting form on the company's website to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		Changes to job roles and responsibilities are communicated to personnel through the entity's SharePoint site.	Inquired of the Director of Information Security regarding changes to job roles and responsibilities to determine that changes to job roles and responsibilities were communicated to personnel through the entity's SharePoint site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the job descriptions on the entity's SharePoint site to determine that changes to job roles and responsibilities were communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Documented procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the entity's SharePoint site.	Inspected the incident response policies and procedures procedure on the entity's SharePoint site to determine that documented procedures for reporting failures, incidents, concerns and other complaints were in place and made available to employees through the entity's SharePoint site.	No exceptions noted.
		The entity's objectives, including changes made to the objectives, are communicated to its personnel through annual meetings.	Inspected the executive management meeting minutes to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through annual meetings.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's third-party agreement delineates the boundaries of the system and describes relevant system components.	Inspected the third-party agreement for a sample of vendors to determine that the entity's third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of external users.	Inspected the third-party agreement for a sample of vendors to determine that the entity's third-party agreement outlined and communicated the terms, conditions and responsibilities of external users.	No exceptions noted.
		The entity's third-party agreement communicates the system commitments and requirements of third-parties.	Inspected the third-party agreement for a sample of vendors to determine that the entity's third-party agreement communicated the system commitments and requirements of third-parties.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the contracts for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
		Documented procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties.	Inspected the process on the entity’s website to determine that documented procedures for reporting failures, incidents, concerns and other complaints were in place and shared with external parties.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the anonymous reporting form on the company’s website to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity communicates to external parties, vendors and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.	Inspected the third-party agreement for a sample of third-parties to determine that the entity communicated to external parties, vendors and service providers the system commitments and requirements related to confidentiality through the use of third-party agreements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.	Inspected the annual company meeting agenda, the organizational chart, and the performance evaluation and review policy to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.
		Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART).	Inspected the annual company meeting agenda to determine that executive management had documented objectives that were SMART.	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the information security risk management policy and the completed risk assessment to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inquired of the Director of Information Security regarding key performance indicators to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the board meeting presentation to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the organizational chart and the Director of Information Security and Manager of Technology job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the budget plan and the annual company meeting presentation to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.
		Entity strategies, objectives and budgets are assessed on a quarterly basis.	Inquired of the Director of Information Security regarding the entity’s strategies, objectives, and budgets to determine that entity strategies, objectives and budgets were assessed on a quarterly basis.	No exceptions noted.
			Inspected the board of directors meeting agenda for a sample of quarters to determine that entity strategies, objectives and budgets were assessed on a quarterly basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures.	Inspected the completed internal controls matrix, the information security policy, and the legal requirements to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures.	No exceptions noted.
		Applicable law, regulation, standard, and legislature requirements are identified and integrated into the entity’s strategies and objectives.	Inspected the annual company meeting agenda, the information security policy, and the legal requirements to determine that applicable law, regulation, standard, and legislature requirements were identified and integrated into the entity’s strategies and objectives.	No exceptions noted.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the information security risk management policy to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks, and defining specified risk tolerances.	Inspected the information security risk management policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks, and defining specified risk tolerances.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inquired of the Director of Information Security regarding the risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
			Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability	Inspected the information security risk management policy and the completed risk assessment to determine that the entity's risk assessment process included: • Identifying the relevant information assets that were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability	No exceptions noted.
		Identified risks are rated using a risk evaluation process.	Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the information security risk management policy and the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the information security risk management policy and the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.	Inspected the information security risk management policy and the completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.	Inspected the completed risk assessment to determine that on an annual basis, management identified and assessed the types of fraud that could impact their business and operations.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Identified fraud risks are reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the completed risk assessment to determine that identified fraud risks were reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered how personnel could engage in or justify fraudulent activities.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT.	Inspected the completed risk assessment to determine that as part of management's assessment of fraud risks, management considered threats and vulnerabilities that arise from the use of IT.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Changes to the regulatory, economic, and physical environment in which the entity operates are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the information security risk management policy and the completed risk assessment to determine that changes to the regulatory, economic, and physical environment in which the entity operates were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the information security risk management policy and the completed risk assessment to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the information security risk management policy and the completed risk assessment to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the information security risk management policy and the completed risk assessment to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IPS configurations and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, a sample alert generated from the FIM software, a sample log extract from the IPS and a sample IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		On a quarterly basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the recording of management's internal audit meeting for a sample of quarters to determine that on a quarterly basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.
		Backup restoration tests are performed on an annual basis.	Inspected the completed backup restoration test results to determine that backup restoration tests were performed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access reviews are performed on at least an annual basis.	Inquired of the Director of Information Security of Technology regarding the logical access reviews to determine that logical access reviews were performed on at least an annual basis.	No exceptions noted.
			Inspected the completed VPN user access review, network user access review, operating system user access review, database user access review and application user access review to determine that logical access reviews were performed on at least an annual basis.	No exceptions noted.
		A third-party performs penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inquired of the Director of Information Security regarding performance evaluations to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the employee evaluation policies and procedures within the employee handbook to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		.	Inspected the completed performance evaluation for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		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 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.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Senior management assesses the results of the compliance, control and risk assessments performed on the environment on a quarterly basis.	Inspected the recording of management's internal audit meeting for a sample of quarters to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment on a quarterly basis.	No exceptions noted.
		Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions.	Inquired of the Director of Information Security regarding vulnerabilities, deviations, and control gaps to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the completed risk assessment to determine that vulnerabilities, deviations, and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical vulnerabilities identified from a vulnerability scan or penetration test to determine that vulnerabilities identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that deviations identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of internal controls that had failed to determine that control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
		Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are documented, investigated, and addressed.	Inquired of the Director of Information Security regarding vulnerabilities, deviations, and control gaps to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were documented, investigated, and addressed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that vulnerabilities, deviations, and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the incident ticket for a sample of critical vulnerabilities identified from a vulnerability scan or penetration test to determine that vulnerabilities identified from the risk and compliance assessments were documented, investigated, and addressed.	No exceptions noted.
			Inspected the incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools, and applications for compliance to determine that deviations identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.
		Management tracks whether vulnerabilities, deviations and control gaps identified as part of the compliance evaluations performed are addressed in a timely manner on a quarterly basis.	Inspected the recording of management's internal audit meeting for a sample of quarters to determine that management tracked whether vulnerabilities, deviations and control gaps identified as part of the compliance evaluations performed were addressed in a timely manner on a quarterly basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	Inspected the completed risk assessment to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	No exceptions noted.
		Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	Inquired of the Director of Information Security regarding control modifications to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the completed risk assessment and the completed internal controls matrix to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of internal controls that had failed to determine that controls within the environment were modified and implemented to mitigate control gaps identified as part of the various evaluations performed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and completed internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the completed internal controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the completed internal controls matrix to determine that management incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inquired of the Director of Information Security regarding risk mitigation strategies to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the information security risk management policy to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of internal controls that had failed to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of vulnerabilities identified from a vulnerability scan or penetration test to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		The business continuity plan and disaster recovery procedures are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that the business continuity plan and disaster recovery procedures were developed and updated on an annual basis.	No exceptions noted.
		The business continuity plan and disaster recovery procedures are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity plan and disaster recovery procedures were tested on an annual basis.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	Inspected the completed internal controls matrix to determine that management documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Information security policies and procedures are documented and made available to employees through the entity's SharePoint site.	Inspected the information security policy and the entity's SharePoint site to determine that information security policies and procedures were documented and made available to employees through the entity's SharePoint site.	No exceptions noted.
		The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats	Inspected the completed internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to: • Restricting access rights to authorized users • Limiting services to what was required for business operations • Authentication of access • Protecting the entity's assets from external threats	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the completed internal controls matrix to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the completed internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the completed risk assessment to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management.	No exceptions noted.
		Management has established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	Inspected the completed internal controls matrix to determine that management established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Information security policies and procedures are documented and made available to employees through the entity's SharePoint site.	Inspected the information security policy and the entity's SharePoint site to determine that information security policies and procedures were documented and made available to employees through the entity's SharePoint site.	No exceptions noted.
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and completed internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.
		Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the completed internal controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the completed internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Process owners and management operate the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and completed internal controls matrix to determine that process owners and management operated the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	No exceptions noted.
		Effectiveness of the internal controls implemented within the environment are evaluated quarterly.	Inspected the executive management meeting minutes for a sample of quarters and the completed internal controls matrix to determine that effectiveness of the internal controls implemented within the environment were evaluated quarterly.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.1	The entity implements logical access security software, infrastructure, and architecture over protected information assets to protect them from security events to meet the entity's objectives.	An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the inventory listing of system assets and components to determine an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policy to determine documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
	Azure AD			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Network administrative access is restricted to the following authorized personnel: • Senior Director of Technology • Director of Information Security • Manager of Technology • DevOps Engineer • Lead DevOps Engineer	Inquired of the Director of Information Security regarding network administrative access to determine that network administrative access was restricted to user accounts accessible by the following authorized personnel: • Senior Director of Technology • Director of Information Security • Manager of Technology • DevOps Engineer • Lead DevOps Engineer	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to user accounts accessible by the following authorized personnel: • Senior Director of Technology • Manager of Technology • SR DevOps Engineer • Senior System Administrator • Senior Software Test Engineer • Infra Support Team	No exceptions noted.
		Network is configured to enforce password requirements that include: • Password history • Password age (maximum) • Password length • Complexity	Inspected the network password settings to determine that the network was configured to enforce password requirements that included: • Password history • Password age (maximum) • Password length • Complexity	No exceptions noted.
		Network users are authenticated via individually assigned user accounts and passwords.	Observed a user login to the network to determine that network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the network account lockout settings to determine that the network account lockout settings were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging settings to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and reviewed as needed.	Inquired of the Director of Information Security regarding network audit logging to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected a sample network audit log extract to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Operating System			
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights for operating systems to determined that operating system user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Operating system administrative access is restricted to authorized personnel.	Inquired of the Director of Information Security regarding operating system administrative access to determine that operating system administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the operating system administrator listing and access rights for a sample of operating systems to determine that operating system administrative access was restricted to authorized personnel.	No exceptions noted.
		Operating systems are configured to enforce password requirements that include: • Password history • Password age (maximum) • Password length • Complexity	Inspected the operating system password configurations to determine that operating systems were configured to enforce password requirements that included: • Password history • Password age (maximum) • Password length • Complexity	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Operating system account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
	Database			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Database administrative access is restricted to the following authorized personnel: • Director of Technology • Senior Director of Technology • Manager of Technology • Senior System Administrator • DevOps Engineer	Inquired of the Director of Information Security regarding database administrative access to determine that database administrative access was restricted to the following authorized personnel: • Director of Technology • Senior Director of Technology • Manager of Technology • Senior System Administrator • Senior DevOps Engineer	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the database administrator listing and access rights to determine that database administrative access was restricted to the following authorized personnel: • Director of Technology • Senior Director of Technology • Manager of Technology • Senior System Administrator • Senior DevOps Engineer	No exceptions noted.
		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.
		Databases are configured to enforce password requirements that include: • Password history • Password maximum age • Password length • Complexity	Inspected the database password settings for a sample of databases to determine that the databases were configured to enforce password requirements that included: • Password history • Password maximum age • Password length • Complexity	No exceptions noted.
		Database users are authenticated via individually assigned user accounts and passwords.	Observed a user login to the database to determine that database users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the database account lockout settings for a sample of databases to determine that database account lockout settings were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Database audit logging settings are in place that include failed logon events.	Inspected the database audit logging settings and a sample database audit log extract for a sample of databases to determine that database audit logging configurations were in place that included failed logon events.	No exceptions noted.
		Database audit logs are maintained and reviewed as needed.	Inquired of the Director of Information Security regarding database audit logging to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected a sample database audit log extract for a sample of databases to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.
	Application (ContractPodAi®)			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application administrative access is appropriately restricted to authorized personnel.	Inquired of the Director of Information Security regarding application administrative access to determine that application administrative access was appropriately restricted to authorized personnel.	No exceptions noted.
			Inspected the application administrator listing and access rights to determine that application administrative access was appropriately restricted to authorized personnel.	No exceptions noted.
		The application is configured to enforce password requirements that include: • Password history • Password maximum age • Password length • Complexity	Inspected the application password settings to determine that application was configured to enforce password requirements that included: • Password history • Password maximum age • Password length • Complexity	No exceptions noted.
		Application users are authenticated via individually assigned user accounts and passwords.	Observed a user login to the application to determine that application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application audit policy settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the application audit logging settings to determine that application audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Application audit logs are maintained and reviewed as needed.	Inquired of the Director of Information Security regarding application audit logging to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected a sample application audit log extract to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
	Remote Access			
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The ability to administer VPN access is restricted to authorized personnel.	Inquired of the Director of Information Security regarding VPN administrative access to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
			Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
		VPN users are authenticated via MFA prior to being granted remote access to the system.	Observed a user authenticate to the VPN to determine that VPN users authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.
			Inspected the VPN authentication settings to determine that VPN users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.
		Data coming into the environment is secured and monitored through the use of firewalls and an IPS.	Inspected IPS configurations, firewall rule sets and the network diagram to determine that data coming into the environment was secured and monitored through the use of firewalls and an IPS.	No exceptions noted.
		A demilitarized zone (DMZ) is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Stored passwords are encrypted.	Inspected encryption configurations for data at rest to determine that stored passwords were encrypted.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the Azure SSE and advanced encryption standard (AES)-256 bit.	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using Azure SSE and AES-256 bit.	No exceptions noted.
		Encryption keys are protected during generation, storage, use, and destruction.	Inspected the encryption policy to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
		Logical access reviews are performed on at least an annual basis.	Inspected the completed VPN user access review, network user access review, operating system user access review, database user access review and application user access review to determine that logical access reviews were performed on at least an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the information security policy containing the hiring procedures, in-scope user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inspected the information security policy containing the termination procedures, in-scope user access listings and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policy to determine documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the information security policy containing the hiring procedures, in-scope user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access to systems is revoked as a component of the termination process.	inspected the information security policy containing the termination procedures, in-scope user access listings and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Logical access reviews are performed on at least an annual basis.	Inspected the completed VPN user access review, network user access review, operating system user access review, database user access review and application user access review to determine that logical access reviews were performed on at least an annual basis.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Director of Information Security regarding access to sensitive resources to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the in-scope systems to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policy to determine documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the information security policy containing the hiring procedures, in-scope user access listings and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inspected the information security policy containing the termination procedures, in-scope user access listings and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Director of Information Security regarding access to sensitive resources to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the in-scope systems to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access reviews are performed on at least an annual basis.	Inspected the completed VPN user access review, network user access review, operating system user access review, database user access review and application user access to determine that logical access reviews were performed on at least an annual basis.	No exceptions noted.
	Network (Azure AD)			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Operating System (Windows)			
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Database (SQL)			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Application			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.	Inspected the media handling and information security policies and procedures to determine policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		Policies and procedures are in place for removal of media storing critical data or software.	Inspected the information media handling policy to determine policies and procedures were in place for removal of media storing critical data or software.	No exceptions noted.
		Data that is no longer required for business purposes is rendered unreadable.	Inquired of the Director of Information Security regarding data disposals to determine data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the information media handling and information security policies to determine data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the service ticket for a sample of requests to dispose of data to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	NAT functionality is utilized to manage internal IP addresses.	Inspected NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		VPN and TLS are used for defined points of connectivity.	Inspected encryption configurations, VPN authentication configurations and digital certificates to determine VPN and TLS were used for defined points of connectivity.	No exceptions noted.
		VPN users are authenticated via MFA prior to being granted remote access to the system.	Inspected the VPN authentication settings to determine that VPN users were authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.
			Observed a user authenticate to the VPN access to determine that VPN users authenticated via MFA prior to being granted remote access to the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Data in transit is encrypted.	Inspected encryption configurations for data in transit and digital certificates to determine that data in transit was encrypted.	No exceptions noted.
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inspected the VPN authentication settings to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed a user authenticate to the VPN access to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Director of Information Security and Information Security Officer regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		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.
		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 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.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The IPS is configured to notify personnel upon intrusion prevention.	Inspected a sample IPS alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.
		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 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.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on a daily basis.	Inspected the centralized antivirus settings to determine that the antivirus software was configured to scan workstations on a daily basis.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the Azure SSE and AES-256 bit.	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using Azure SSE and AES-256 bit.	No exceptions noted.
		A DMZ is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media configurations to determine that the use of removable media was prohibited.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Logical access to stored data is restricted to the following authorized personnel: • Senior Director of Technology • Manager of Technology • DevOps Engineer • Lead DevOps Engineer • Manager of Technology	Inquired of the Director of Information Security regarding access to stored data to determine that logical access to stored data was restricted to the following authorized personnel: • Senior Director of Technology • Manager of Technology • DevOps Engineer • Lead DevOps Engineer • Manager of Technology	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to the following authorized personnel: • Senior Director of Technology • Manager of Technology • DevOps Engineer • Lead DevOps Engineer • Manager of Technology	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The ability to restore backed up data is restricted to authorized personnel.	Inquired of the Director of Information Security regarding the ability to restore backed up data to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
			Inspected the list of users with the ability to restore backup media to determine that the ability to restore backed up data was restricted to authorized personnel.	No exceptions noted.
		The entity secures its environment a using multi-layered defense approach that includes firewalls, an IPS, antivirus software and a DMZ.	Inspected the network diagram, IPS configurations, firewall rule sets, antivirus settings and DMZ settings to determine that the entity secured its environment a using multi-layered defense approach that included firewalls, an IPS, antivirus software and a DMZ.	No exceptions noted.
		VPN and TLS are used for defined points of connectivity.	Inspected encryption configurations, VPN authentication configurations and digital certificates to determine VPN and TLS were used for defined points of connectivity.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inspected the VPN authentication settings to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		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.
		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 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.
		NAT functionality is utilized to manage internal IP addresses.	Inspected NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The IPS is configured to notify personnel upon intrusion prevention.	Inspected a sample IPS alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the Azure SSE and AES-256 bit.	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using Azure SSE and AES-256 bit.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected encryption configurations for backup media to determine that backup media was stored in an encrypted format.	No exceptions noted.
		Data in transit is encrypted.	Inspected encryption configurations for data in transit and digital certificates to determine that data in transit was encrypted.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the information media handling policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media configurations to determine that the use of removable media was prohibited.	No exceptions noted.
		Mobile devices are protected through the use of secured, encrypted connections.	Inspected the VPN encryption configurations to determine that mobile devices were protected through the use of secured, encrypted connections.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	A warning notification appears when an employee attempts to download an application or software.	Inspected the warning notification received when an employee attempted to download an application or software to determine that a warning notification appeared when an employee attempted to download an application or software.	No exceptions noted.
		The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Director of Information Security and regarding access to migrate changes 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.
		FIM software is in place to ensure only authorized changes are deployed into the production environment.	Inspected FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The FIM software is configured to notify IT personnel via email alert when a change to the production application code files is detected.	Inspected FIM configurations and a sample alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via email alert when a change to the production application code files was detected.	No exceptions noted.
		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.
		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 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.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on a daily basis.	Inspected the centralized antivirus settings to determine that the antivirus software was configured to scan workstations on a daily basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Information assets, software, hardware, tools, and applications introduced into the environment are scanned for vulnerabilities and malware prior to implementation into the environment.	Inspected the technical vulnerability management policy to determine that information assets, software, hardware, tools, and applications introduced into the environment were scanned for vulnerabilities and malware prior to implementation into the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Management has defined configuration standards in the information security policies and procedures.	Inspected the information security management system policy to determine that management had defined configuration standards in the information security policies and procedures.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IPS configurations and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, a sample alert generated from the FIM software, a sample log extract from the IPS and a sample IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The IPS is configured to notify personnel upon intrusion prevention.	Inspected a sample IPS alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.
		FIM software is in place to ensure only authorized changes are deployed into the production environment.	Inspected FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via email alert when a change to the production application code files is detected.	Inspected FIM configurations and a sample alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via email alert when a change to the production application code files was detected.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media configurations to determine that the use of removable media was prohibited.	No exceptions noted.
		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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 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.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security management system policy and incident response policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		Vulnerability scans are performed on a monthly basis on the environment to identify control gaps and vulnerabilities.	Inspected the completed vulnerability scan for a sample of months to determine that vulnerability scans were performed monthly on the environment to identify control gaps and vulnerabilities.	No exceptions noted.
		A third-party performs penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Documented incident response policies and procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management to determine that documented incident response and procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security management system policy and incident response policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IPS configurations and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, a sample alert generated from the FIM software, a sample log extract from the IPS and a sample IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		An IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected IPS configurations to determine that an IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IPS is configured to notify personnel upon intrusion prevention.	Inspected a sample IPS alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	No exceptions noted.
		FIM software is in place to ensure only authorized changes are deployed into the production environment.	Inspected FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The FIM software is configured to notify IT personnel via email alert when a change to the production application code files is detected.	Inspected FIM configurations and a sample alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via email alert when a change to the production application code files was detected.	No exceptions noted.
		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.
		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 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.
		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 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.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The antivirus software is configured to scan workstations on a daily basis.	Inspected the centralized antivirus settings to determine that the antivirus software was configured to scan workstations on a daily basis.	No exceptions noted.
		The entity's third-party agreement requires third-parties to implement detective controls and provide notice if the third-party's environment is compromised.	Inspected the third-party agreement master template to determine that the entity's third-party agreement required third-parties to implement detective controls and provide notice if the third-party's environment was compromised.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media configurations to determine that the use of removable media was prohibited.	No exceptions noted.
		Vulnerability scans are performed on a monthly basis on the environment to identify control gaps and vulnerabilities.	Inspected the completed vulnerability scan for a sample of months to determine that vulnerability scans were performed monthly on the environment to identify control gaps and vulnerabilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Network AD			
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the network account lockout settings to determine that network account lockout settings were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging settings to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Azure AD audit logs are maintained and reviewed as needed.	Inquired of the Director of Information Security regarding network audit logging to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected a sample network audit log extract to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Operating System			
		Operating system account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Operating system audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the operating system audit logging settings to determine that operating system audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Operating system audit logs are maintained and reviewed as-needed.	Inspected a sample operating system audit log extract to determine that operating system audit logs were maintained and reviewed as-needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Database (SQL)			
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the database account lockout settings for a sample of databases to determine that database account lockout settings were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Database audit logging settings are in place that include failed logon events.	Inspected the database audit logging settings and a sample database audit log extract for a sample of databases to determine that database audit logging configurations were in place that included failed logon events.	No exceptions noted.
		Database audit logs are maintained and reviewed as needed.	Inquired of Director of Information Security regarding database audit logging to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected a sample database audit log extract for a sample of databases to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Application (ContractPodAi®)			
		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.
		Application audit policy settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the application audit logging settings to determine that application audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Application audit logs are maintained and reviewed as needed.	Inquired of Director of Information Security regarding application audit logging to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected a sample application audit log extract to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this criterion is the responsibility of the subservice organization. Refer to the “Subservice Organizations” section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response policies and procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management to determine that documented incident response policies and procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		The incident response policies and procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident response policies and procedures to determine that the incident response policies and procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Director of Information Security regarding security incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected incident response policies and procedures to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for the population of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Director of Information Security 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 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Identified incidents are reviewed, monitored, and investigated by an incident response team.	Inquired of the Director of Information Security regarding security incidents to determine that identified incidents were reviewed, monitored, and investigated by an incident response team.	No exceptions noted.
			Inspected incident response policies and procedures to determine that identified incidents were reviewed, monitored, and investigated by an incident response team.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were reviewed, monitored, and investigated by an incident response team.	No exceptions noted.
		Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Inquired of the Director of Information Security regarding security incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident management process to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the incident response policies and procedures to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented incident response policies and procedures for reporting security incidents are in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident response policies and procedures to determine that documented incident response policies and procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the supporting incident ticket for a sample of incidents to determine incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		Documented incident response policies and procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the incident response policies and procedures to determine that documented incident response policies and procedures were in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.
		Critical security incidents that result in a service/business operation disruption are communicated to those affected through incident tickets.	Inquired of the Director of Information Security regarding critical incidents to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through incident tickets.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through incident tickets.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incidents that resulted in a service/business operation disruption to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through incident tickets.	Testing of the control activity disclosed that there were no critical security incidents that resulted in a service/business operation disruption.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Director of Information Security regarding security incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected incident response policies and procedures to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Inquired of the Director of Information Security regarding security incidents to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The risks associated with identified vulnerabilities are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the completed risk assessment to determine that the risks associated with identified vulnerabilities were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		The incident response policies and procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident response policies and procedures to determine that the incident response policies and procedures were reviewed at least annually for effectiveness.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Change management requests are opened for incidents that require permanent fixes.	Inspected the change management policies and procedures to determine that change management requests were required to be opened for incidents that required permanent fixes.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	Inspected the information security, incident, and change management policies and procedures for critical systems to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures within Information Security Policy to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		Backup restoration tests are performed on an annual basis.	Inspected the completed backup restoration test results to determine that backup restoration tests were performed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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.
		The business continuity plan and disaster recovery procedure are tested on an annual basis.	Inspected the completed business continuity plan and disaster recovery procedure test results to determine that the business continuity plan and disaster recovery procedure were tested on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	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.
		FIM software is in place to ensure only authorized changes are deployed into the production environment.	Inspected FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		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.
		The FIM software is configured to notify IT personnel via email alert when a change to the production application code files is detected.	Inspected FIM configurations and a sample alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via email alert when a change to the production application code files was detected.	No exceptions noted.
		Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.	Inspected the Information Security Management System Policy to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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.
		System change requests are documented and tracked in a ticketing system.	Inspected the supporting change ticket for a sample of change tickets to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the supporting change ticket for a sample of change tickets to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.
		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 change tickets 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.
		The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Director of Information Security and regarding access to migrate changes to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			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.
		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.
		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 settings 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.
		System changes are communicated to both affected internal and external users.	Inspected the internal and external communications for change notice emails to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate development, QA, staging, and production environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity creates test data using data masking software that replaces confidential information with test information during the change management process.	Inspected the system environments 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.
		Changes implemented into the production environment trigger an alert to affected users.	Inspected the change control software settings and a sample alert to determine that changes implemented into the production environment triggered an alert to affected users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Documented policies and procedures are in place to guide personnel in performing risk mitigation activities.	Inspected the information security risk management policy to determine that documented policies and procedures were in place to guide personnel in performing risk mitigation activities.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the information security risk management policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inquired of the Director of Information Security regarding the risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
			Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Identified risks are rated using a risk evaluation process.	Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process.	No exceptions noted.
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the information security risk management policy and the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the information security risk management policy and the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	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 management policy 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.
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the vendor management policy to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.
		Identified third-party risks are evaluated by management.	Inspected the vendor management policy to determine that identified third-party risks were evaluated by management.	No exceptions noted.
			Inspected the completed vendor risk assessment for a sample of vendors to determine that identified third-party risks were evaluated by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's third-party agreement outlines and communicates: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels	Inspected the third-party agreement master template to determine that the entity's third-party agreement outlined and communicated: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	No exceptions noted.
			Inspected the third-party agreement for a sample of vendors to determine that the entity's third-party agreement outlined and communicated: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 vendors 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.
		A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements.	Inspected vendor management policy 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 vendors 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.
		Management has assigned responsibility and accountability for the management of risks associated with third-parties to appropriate personnel.	Inspected the organizational chart and the job descriptions for personnel responsible for compliance activities to determine that management assigned responsibility and accountability for the management of risks associated with third-parties to appropriate personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has established exception handling procedures for services provided by third-parties.	Inspected the vendor management policy to determine that management established exception handling procedures for services provided by third-parties.	No exceptions noted.
		The entity has documented procedures for addressing issues identified with third-parties.	Inspected the vendor management policy to determine that the entity documented procedures for addressing issues identified with third-parties.	No exceptions noted.
		The entity's third-party agreement outlines and communicates confidentiality commitments and requirements.	Inspected the third-party agreement master template to determine that the entity's third-party agreement outlined and communicated confidentiality commitments and requirements.	No exceptions noted.
			Inspected the third-party agreement for a sample of vendors to determine that the entity's third-party agreement outlined and communicated confidentiality commitments and requirements.	No exceptions noted.
		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 vendors to determine that management assessed the compliance of privacy commitments and requirements of third-parties at least annually.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IPS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, a sample alert generated from the FIM software, a sample log extract from the IPS and a sample IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		Processing capacity is monitored 24x7x365.	Inspected the monitoring tool configurations to determine that processing capacity was monitored 24x7x365.	No exceptions noted.
		Processing capacity is automatically balanced in real-time.	Inspected the autoscaling configurations to determine that processing capacity was automatically balanced in real-time.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Environmental threats that could impair the availability of the system are considered and identified as a part of the risk assessment process.	Inspected the completed risk assessment to determine that environmental threats that could impair the availability of the system were considered and identified as a part of the risk assessment process.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Risks relating to environmental threats identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the completed risk assessment to determine that risks relating to environmental threats identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		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 and configurations for critical systems 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.
			Inspected the 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.
		When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure.	Inspected backup configurations and a sample backup alert 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.
		Data backed up is replicated to a secondary region in real-time.	Inspected backup replication configurations to determine that data backed up was replicated to a secondary region in real-time.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Redundant architecture is in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	Inspected the business continuity and disaster recovery plans and network diagram to determine that redundant architecture was in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	No exceptions noted.
		The disaster recovery plan includes moving the business operations and supporting systems to a hot site.	Inspected the business continuity and disaster recovery plans to determine that the disaster recovery plan included moving the business operations and supporting systems to a hot site.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the “Subservice Organizations” section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.	Inspected the business continuity and disaster recovery plans to determine that a business continuity plan was documented and in place that outlined the range of disaster scenarios and steps the business would take in a disaster to ensure the timely resumption of critical business operations.	No exceptions noted.
		The business continuity plan and disaster recovery procedure is tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity plan was tested on an annual basis.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Backup restoration tests are performed on an annual basis.	Inspected the completed backup restoration test results to determine that backup restoration tests were performed on an annual basis.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Documented confidentiality policies and procedures are in place that include the following: • Defining, identifying and designating information as confidential • Storing confidential information • Protecting confidential information from erasure or destruction • Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed	Inspected the information security policy and the asset management policy to determine that documented confidential policies and procedures were in place that included: • Defining, identifying and designating information as confidential • Storing confidential information • Protecting confidential information from erasure or destruction • Retaining confidential information for only as long as it is required to achieve the purpose for which the data was collected and processed	No exceptions noted.
		An inventory log is maintained of assets with confidential data.	Inspected the inventory log to determine that an inventory log was maintained of assets with confidential data.	No exceptions noted.
		Confidential information is maintained in locations restricted to those authorized to access.	Inquired of the Director of Information Security regarding access to confidential information to determine that confidential information was maintained in locations restricted to those authorized to access.	No exceptions noted.
			Inspected the access permissions for a sample file marked as confidential to determine that confidential information was maintained in locations restricted to those authorized to access.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Confidential information is protected from erasure or destruction during the specified retention period.	Inspected the confidentiality policies and procedures to determine that confidential information was protected from erasure or destruction during the specified retention period.	No exceptions noted.
			Inspected the supporting ticket request for a sample of data disposals to determine that confidential information was protected from erasure or destruction during the specified retention period.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Documented data destruction policies and procedures are in place that include the following: • Identifying confidential information requiring destruction when the end of the retention period is reached • Erasing or destroying confidential information that has been identified for destruction	Inspected the media handling policy, information security policy and asset management policy to determine that documented data destruction policies and procedures were in place that included: • Identifying confidential information requiring destruction when the end of the retention period was reached • Erasing or destroying confidential information that has been identified for destruction	No exceptions noted.
		An inventory log is maintained of assets with confidential data, and as confidential data meets the retention period, the data is destroyed or purged.	Inspected the inventory log to determine that an inventory log was maintained of assets with confidential data, and as confidential data met the retention period, the data was destroyed or purged.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY				
C1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity purges confidential data after it is no longer required to achieve the purpose for which the data was collected and processed.	Inquired of the Director of Information Security regarding purging of confidential data to determine that the entity purged confidential data after it was no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.
			Inspected the data disposal policies and procedures within the information security policy to determine that the entity purged confidential data after it was no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.
			Inspected the supporting ticket request for a sample of data disposals to determine that the entity purged confidential data after it was no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.