A-LIGN

MealSuite, Inc.

Type 2 SOC 2

2024

MEALSUITE

A-LIGN.COM

REPORT ON MEALSUITE, INC.'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY

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

February 1, 2024 to October 31, 2024

Table of Contents

SECTION 1

ASSERTION OF MEALSUITE, INC. MANAGEMENT

ASSERTION OF MEALSUITE, INC. MANAGEMENT

December 15, 2024

We have prepared the accompanying description of MealSuite, Inc.'s ('MealSuite' or 'the Company') Cloud-Based FoodService Software Services System titled "MealSuite, Inc.'s Description of Its Cloud-Based FoodService Software Services System throughout the period February 1, 2024 to October 31, 2024" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Cloud-Based FoodService Software Services System that may be useful when assessing the risks arising from interactions with MealSuite's system, particularly information about system controls that MealSuite has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security (applicable Trust Services Criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

MealSuite uses Digital Realty Trust, Inc. ('Digital Realty' 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 MealSuite, to achieve MealSuite's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents MealSuite's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of MealSuite'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 MealSuite, to achieve MealSuite's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents MealSuite's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of MealSuite's controls.

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

a. the description presents MealSuite's Cloud-Based FoodService Software Services System that was designed and implemented throughout the period February 1, 2024 to October 31, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period February 1, 2024 to October 31, 2024, to provide reasonable assurance that MealSuite'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 MealSuite's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period February 1, 2024 to October 31, 2024, to provide reasonable assurance that MealSuite'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 MealSuite's controls operated effectively throughout that period.

Sean Rowe
President & CEO
MealSuite, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: MealSuite, Inc.

Scope

We have examined MealSuite's accompanying description of its Cloud-Based FoodService Software Services System titled "MealSuite, Inc.'s Description of Its Cloud-Based FoodService Software Services System throughout the period February 1, 2024 to October 31, 2024" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 1, 2024 to October 31, 2024, to provide reasonable assurance that MealSuite's service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security (applicable Trust Services Criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

MealSuite uses Digital Realty 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 MealSuite, to achieve MealSuite's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents MealSuite's controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of MealSuite'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 MealSuite, to achieve MealSuite's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents MealSuite's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of MealSuite'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

MealSuite 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 MealSuite's service commitments and system requirements were achieved. MealSuite has provided the accompanying assertion titled "Assertion of MealSuite, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. MealSuite 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 MealSuite's Cloud-Based FoodService Software Services System that was designed and implemented throughout the period February 1, 2024 to October 31, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period February 1, 2024 to October 31, 2024, to provide reasonable assurance that MealSuite'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 MealSuite's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period February 1, 2024 to October 31, 2024, to provide reasonable assurance that MealSuite'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 MealSuite'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 MealSuite, user entities of MealSuite's Cloud-Based FoodService Software Services System during some or all of the period February 1, 2024 to October 31, 2024, business partners of MealSuite subject to risks arising from interactions with the Cloud-Based FoodService Software 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
December 15, 2024

SECTION 3

MEALSUITE, INC.'S DESCRIPTION OF ITS CLOUD-BASED FOODSERVICE SOFTWARE SERVICES SYSTEM THROUGHOUT THE PERIOD FEBRUARY 1, 2024 TO OCTOBER 31, 2024

OVERVIEW OF OPERATIONS

Company Background

Founded in 1984 as a technology consulting business, MealSuite (formerly SureQuest) has developed into a Food Service Management leader, serving clients throughout North America.

Today MealSuite's web-based software platform serves over 3,000 healthcare operators, empowering them to automated and digitize their operations to ensure compliance, reduce risk and deliver the highest quality of care to patients and residents.

Description of Services Provided

MealSuite's web-based food service management software platform is scalable to assist various sizes of organizations. Whether a client is looking to operate in an entirely automated and paperless system or simply conduct a costing or nutrient analysis of an existing menu, MealSuite's modules can be turned on and off based on licensing. Modules include:

- Menu Management
- Nutritional Analysis - With integrations to major food manufacturers to ensure the most recent and accurate data
- Menu Costing - With integration with distributor partners to automate costing
- Inventory Management
- Meal Service Tools - Reports to meet compliance at time of delivery to residents or patients
- Digital Menu Boards
- Production Tools - Recipe scaling and forecasting to reduce food waste and ensure consistency
- Procurement - With integrations to major distributor partners
- People and Patient Management - With optional integration into customer Electronic Health Record (EHR)/Electronic Medical Record (EMR) systems
- Point of Sale
- MealSuite Touch - Add-on iDevice Operating System (IOS)/Android application, enabling customers to go paperless

In addition to the web-based platform provided to customers, MealSuite also sells equipment to support on-site operations. The equipment is manufactured, certified, and warrantied by third-party vendors. Equipment includes but is not limited to:

- Digital touch-screen Menu Boards
- Tablets and portable device for use in meal ordering, inventory, etc.
- Sensors to monitor food, refrigerator, and freezer temperatures
- Thermal Printers, Food Scales, Cash Drawers and other accessories as required

Principal Service Commitments and System Requirements

MealSuite designs its processes and to meet its objectives for its foodservice automation services. Those objectives are based on the service commitments that MealSuite makes to clients, the laws and regulations that govern the provision of the industry, and the financial, operational, and compliance requirements that MealSuite has established for the services. The foodservice automation services of MealSuite are subject to the security and privacy requirements of the Health Insurance Portability, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which MealSuite delivers services.

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

- Security principles within the fundamental designs of MealSuite's software are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Best practices are followed to ensure the protection of clients' data.

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

Components of the System

Infrastructure

MealSuite utilizes a variety of hardware and software vendors to ensure the highest level of security and up-time for both internal and external customers. These vendors include system virtualization, firewalls, security-as-a-service, and dev-ops-as-a-service. MealSuite's internal systems are cloud based with remote access capabilities globally for employees, reducing dependencies on internal networks and offices.

Software

Primary software used to provide MealSuite's Cloud-Based FoodService Software Services System includes the use of open-sourced Linux Based Technologies including PostgreSQL, Ubuntu, Ruby On Rails, Redis and Angular. Third-party software vendors including Salesforce, Microsoft Office, JIRA and Zendesk are utilized to support the customer and internal teams.

People

MealSuite is owned by CloudStorm Ventures, where it gains access to shared resources such as Human Resources, Marketing, Software Engineering, Information Technology (IT) (Administration and Security) and Finance.

There is a dedicated team of 130+ individuals that are not shared with other portfolio companies, with a further group of 40 resources that may service one or more organization within the portfolio.

<u>Finance Operations</u>

Responsible for payroll administration, accounts payable, accounts receivable, tax and financial filings. A third-party firm is engaged for payroll and compliance in Vietnam.

<u>Human Resources</u>

Compliance, recruiting, people operations, on-boarding and benefits administration.

<u>Sales and Marketing</u>

Product sales, marketing and partner channel support.

Nutrition Services

A team of registered dieticians or similar qualification, responsible for quality assurance (QA) and the creation and maintenance of starting base recipes and menus for customers. This team are also engaged to assist customers with data entry and initial data setup of the system.

Product Management

Responsible for planning the software release roadmap, collecting customer feedback, feature design and validation.

Engineering

Software development, Artificial Intelligence (AI) and Machine learning, manual and automated QA testing teams and database management.

Customer Support

Technical and functional support of the software and hardware platforms. Available during regular business hours with 24/7 coverage for any critical issues outside regular hours.

Onboarding

Responsible for the training and successful onboarding of new customer facing projects.

Project Management

A dedicated project management office with oversight of internal corporate projects, privacy, risk and security compliance.

IT Operations

Employee hardware administration, office networks, telephone system management, internal user access rights management, network and device security monitoring and support of internal tools used by staff.

Data

Data, as defined by MealSuite, constitutes the following:

- Resident and Patient Data
- Food Nutrient Data
- Distributor/Procurement Vendor Data
- Compiled Reports
- Menus and Recipes

People Data is stored in the MealSuite system to provide clients with the opportunity to offer and serve foods that are appropriate for each person's specific allergies, dislikes, preferences, and diet order.

People Data is input into food service provider's application through a number of secure methods:

1. Manually by a user (Password and role authorization required).
2. Secure File Transfer Protocol (SFTP).
3. Secure Websites through Application Programming Interface (API) or Webservices transactions from secure Patient Information Systems.

Output Reports of people information are available in Portable Document Format (PDF) or Excel format, the availability of these reports can only be generated directly from the password protected MealSuite application.

Nutrient Data is stored in the MealSuite system to provide clients with detailed nutritional information that can be utilized to ensure that the recommended dietary allowance for each resident is being met, or that the information is readily available to their clients so that they can make their own informed decisions about their dietary choices.

Nutrient Data is provided from either an authorized government website or provided from a trusted Data Provider. Nutrient data is then imported into the MealSuite Master Data system and reviewed by the Nutrition Services team.

Output Reports are available in PDF or Excel format and can only be generated directly from the password protected MealSuite application. Nutrient Data can also be transmitted to a client's website using a MealSuite developed API connections secured by trusted security certificates.

Vendor Product Data is stored in the MealSuite system to provide the opportunity to cost their recipe and food data.

Master Recipe and Menu Data is available to clients within their database.

Facility specific Recipe and Menu data can only be input manually by the user directly into the password protected MealSuite database.

Processes, Policies and Procedures

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

Physical Security

MealSuite utilizes off-site datacenter providers for the storage and environmental security of infrastructure and confidential data. Office facilities contain paper records of documents for the purpose of financial or employment audits. Offices in North America are secured by key fob or virtual keys on mobile devices, rooms that contain network equipment or confidential records are secured by an additional hard lock and key. Offices have cameras that record upon any motion.

The in-scope system and supporting infrastructure are hosted by Digital Realty. As such, Digital Realty is responsible for the physical security controls for the in-scope system. Refer to the "Subservice Organizations" section below for controls managed by Digital Realty.

Logical Access

MealSuite uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists.

Internal corporate assets are tracked, and owners are required to authorize access. Period reviews are completed of access lists. User accounts for internal corporate tools and network are managed through Active Directory. Upon termination, user accounts are locked which immediately block access to Virtual Private Network (VPN) and any confidential materials. Third-party tools monitor systems to track failed login attempts or attempts to breach security systems and alert management.

MealSuite application assigns user access right ownerships to the owner of the account. Ownership is assigned based on the software agreement. The owner has the right to request additional users access, change passwords and implement their own internal security policies. MealSuite sends period lists of user accounts to corporations for review. Single Sign-On (SSO) services are also available for corporations that wish to implement them.

Computer Operations - Backups

MealSuite has implemented a number of safeguards to protect data. Two datacenters operate in active/active mode with log-shipping between the facilities. In the event off a catastrophic failure, services can be moved within 5 minutes to the secondary location.

To protect against data corruption a full nightly backup is shipped off-site to Amazon Web Services Simple Storage Service (S3).

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.

MealSuite monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches SLAs.

MealSuite evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers.

Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center rack space
- Disk storage
- Computational Resources
- Network bandwidth

The IT team are responsible for ensuring systems are patched and secured.

Change Control

MealSuite 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, QA 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. QA 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. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

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

Data Communications

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

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 hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party tool 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 tool 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.

Boundaries of the System

The scope of this report includes the Cloud-Based FoodService Software Services System performed in the Dallas, Texas (United States); Cambridge, Ontario (Canada); and Ho Chi Minh City (Vietnam) facilities.

This report does not include the data center hosting services provided by Digital Realty.

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 MealSuite's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of MealSuite's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

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

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

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

Management's Philosophy and Operating Style

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

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

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- Executive management directly work with innovative clients and their frontline teams to ensure MealSuite meets their requirements and are delivery effective solutions.

Organizational Structure and Assignment of Authority and Responsibility

MealSuite'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.

MealSuite'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.

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

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.
- Role descriptions are available for review by employees.
- Employee growth tracks and career ladders are published to employees globally.

Human Resources Policies and Practices

MealSuite'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 quality personnel who ensures the service organization is operating at maximum efficiency. MealSuite's Human Resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on at least an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.
- Job Tracks are in place and publicly available within the organization to clearly articulate requirements to move to a higher position.
- Employees are encouraged to cross-train and pursue their interests with the opportunity for department transfers and role changes.
- Weekly touch-points are conducted via Employee Engagement platform (Lattice) to ensure on-going success.

Risk Assessment Process

MealSuite's risk assessment process identifies and manages risks that could potentially affect MealSuite's ability to provide reliable services to clients' organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. MealSuite 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 MealSuite, 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
- Data Security and Privacy - unauthorized access to clients' data

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of MealSuite's food service automation system; as well as the nature of the components of the system result in risks that the criteria will not be met. MealSuite 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, MealSuite'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 are an integral component of MealSuite'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 MealSuite, 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, town hall meetings are held monthly to provide staff with updates on the company and key issues affecting the organization and its employees.

Senior executives lead the town hall 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 MealSuite personnel via email messages.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. MealSuite'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

MealSuite's management conducts QA monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in MealSuite's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of MealSuite's personnel.

Reporting Deficiencies

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

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

All Common Criteria/Security was applicable to the MealSuite Cloud-Based FoodService Software Services System.

Subservice Organizations

This report does not include the data center hosting services provided by Digital Realty.

Subservice Description of Services

MealSuite contracts with Digital Realty to host primary infrastructure within their data centers.

Complementary Subservice Organization Controls

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

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

Subservice Organization - Digital Realty		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Access to the card access control system used to grant, modify, or revoke access rights is restricted to authorized personnel based on job responsibility. This includes members from the IT Service Desk, Data Center Infrastructure (DCI), and Data Center Operations (DCO) teams.
		Physical access to data center is controlled and authenticated by one or more of the following physical access mechanisms: access cards, biometrics, pin pad, or manual sign-in procedures.
		Access cards for unescorted technicians or contractors are configured to expire at the end of a specific time period.
		Colocation customer access changes (for new or existing access) are provided based on approval from an authorized customer representative. The physical access is granted by an authorized DCO personnel.
		Physical access to data center is granted based on an employee's job responsibilities and authorization from DCO management.
		The IT Service Desk or DCO teams remove data center access for terminated employee upon notification by the Human Resources team.
		On a quarterly basis, the Information Security and DCO teams perform a review of employees and customer who have access to the data centers. Access rights are modified or disabled, as necessary.
		Surveillance cameras are placed at entrances and other key locations within the data center. Video surveillance footage is recorded and retained for at least 90 days.
		Colocation customer servers are physically segregated in locked cabinets within a designated section of the data center facility. Colocation customers are provided a key or combination code to gain access.

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

- Reviewing and reconciling output reports

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

COMPLEMENTARY USER ENTITY CONTROLS

MealSuite'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 MealSuite's services to be solely achieved by MealSuite control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of MealSuite'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 MealSuite.
2. User entities are responsible for notifying MealSuite of changes made to technical or administrative contact information.
3. User entities are responsible for ensuring the supervision, management, and control of the use of MealSuite services by their personnel.
4. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize MealSuite's services.
5. User entities are responsible for immediately notifying MealSuite of any actual or suspected information security breaches, including compromised user accounts.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security Category)
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.

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 MealSuite's description of the system. Any applicable Trust Services Criteria that are not addressed by control activities at MealSuite 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 MealSuite was limited to the Trust Services Criteria, related criteria and control activities specified by the management of MealSuite and did not encompass all aspects of MealSuite'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; and
- 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 policies, directives, guidelines, and the employee handbook.	Inspected the employee handbook, information security policies and procedures and the entity's Intranet to determine that core values were communicated from executive management to personnel through policies, directives, guidelines, and 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.	Inspected the signed employee handbook acknowledgment for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.
		Upon hire, personnel are required to sign a confidentiality agreement.	Inspected the signed confidentiality agreement for a sample of new hires to determine that upon hire, personnel were required to sign a confidentiality agreement.	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 hire, personnel are required to complete a background check.	Inspected the background check policies and procedures and 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.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on at least an annual basis.	Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on at least an annual basis.	No exceptions noted.
		Sanction policies, which include suspension and termination, are in place for employee misconduct.	Inspected the sanction policies to determine that sanction policies, which include suspension and termination, were in place for employee misconduct.	No exceptions noted.
		An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Inspected the anonymous reporting hotline to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	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**
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 for a sample of executive management 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 roles to determine that executive management defined and documented the skills and expertise needed among its members.	No exceptions noted.
		Executive management evaluates the skills and expertise of its members at least annually.	Inspected the completed performance evaluation form for a sample of executive management members to determine that executive management evaluated the skills and expertise of its members at least annually.	No exceptions noted.
		Executive management maintains independence from those that operate the key controls 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.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected the internal management meeting invite and agenda to determine that executive management met annually with operational management to assess the effectiveness and performance of internal 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**
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the completed internal controls matrix to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.
			Inspected the internal management meeting invite and agenda to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	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.
		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 organizational 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 Intranet.	Inspected the job description for a sample of job roles and the entity's Intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's Intranet.	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 job descriptions annually and makes updates, if necessary.	Inspected the revision history of the job description for a sample of job 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 acknowledgment for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.
		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 established proper segregations of duties for key job functions and roles within the organization.	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 employee performance evaluation policies and procedures and competency and training requirements policies and procedures 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.

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**
		Performance and conduct evaluations are performed for personnel on at least an annual basis.	Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on at least an annual basis.	No exceptions noted.
		The entity evaluates the competencies and experience of candidates prior to hiring.	Inspected the resume for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	No exceptions noted.
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.	Inspected the job description for a sample of job roles and the resume for a sample of new hires to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.	No exceptions noted.
		The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives.	Inspected the job opening postings and requisition request worksheet to determine that the entity had a recruiting department that was responsible for attracting individuals with competencies and experience that aligned with the entity's goals and objectives.	No exceptions noted.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the HIPAA training tracker to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	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 completed training for a sample of current employees to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No exceptions noted.
		Executive management uses an outside vendor to assist with its continued training of employees.	Inspected the information security and awareness training materials to determine that executive management used an outside vendor to assist with its continued training of employees.	No exceptions noted.
		Executive management tracks and monitors compliance with training requirements.	Inspected the HIPPA training tracker to determine that executive management tracked and monitored compliance with training requirements.	No exceptions noted.
		As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations as it relates to their job role and responsibilities.	Inspected the employee performance evaluation policies and procedures to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations as it relates to their job role and responsibilities.	No exceptions noted.
		Upon hire, personnel are required to complete a background check.	Inspected the background check policies and procedures and 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.

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**
CC1.5	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 Intranet.	Inspected the job description for a sample of job roles and the entity's Intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's Intranet.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook.	Inspected the signed employee handbook acknowledgment for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook 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**
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance evaluation policies and procedures and competency and training requirements policies and procedures 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.
		Executive management has established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities.	Inspected the employee performance evaluation policies and procedures to determine that executive management established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on at least an annual basis.	Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on at least 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**
		As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations and performs disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	Inspected the employee performance evaluation policies and procedures to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations and performed disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	No exceptions noted.
		Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary.	Inspected the revision history of the job description for a sample of job roles to determine that executive management reviewed the job requirements and responsibilities documented within job descriptions annually and made updates, if necessary.	No exceptions noted.
		Sanction policies, which include suspension and termination, are in place for employee misconduct.	Inspected the sanction policies to determine that sanction policies, which include 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.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's Intranet.	Inspected the information security policies and procedures, job description for a sample of job roles and the entity's Intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's Intranet.	No exceptions noted.
		Required nutritional fields must be entered into the system. Any missing fields are reviewed in exceptions summary reports.	Inspected the exceptions check tool to determine that required nutritional fields had to be entered into the system, and that any missing fields were reviewed in exceptions summary reports.	No exceptions noted.
		Clients review exceptions summary reports to resolve any known data discrepancies.	Inspected the exceptions check tool to determine that clients reviewed exceptions summary reports to resolve any known data discrepancies.	No exceptions noted.
		Data entered into the system is reviewed for completeness and accuracy.	Inspected the exceptions check tool to determine that data entered into the system was reviewed for completeness and accuracy.	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, Intrusion Prevention System (IPS) configurations, encryption methods and configurations and VPN authentication configurations to determine that data entered into the system, processed by the system and output from the system was protected from unauthorized access.	No exceptions noted.
		Data and information critical to the system is assessed annually for relevance and use.	Inspected the data criticality report to determine that data and information critical to the system was assessed annually for relevance and use.	No exceptions noted.
		Data is only retained for as long as required to perform the required system functionality, service or use.	Inquired of the Chief Executive Officer regarding data destruction to determine that data was only retained for as long as required to perform the required system functionality, service or use.	No exceptions noted.
			Inspected the record retention and destruction policies and procedures to determine that data was only retained for as long as required to perform the required system functionality, service or use.	No exceptions noted.
			Inspected the destruction certification for a sample of data destruction requests to determine that data was only retained for as long as required to perform the required system functionality, service or use.	Testing of the control activity disclosed that there were no data destruction requests during the review period.

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**
CC2.2	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 Intranet.	Inspected the job description for a sample of job roles and the entity's Intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's Intranet.	No exceptions noted.
		The entity's policies and procedures and employee handbook are made available to employees through the entity's Intranet.	Inspected the entity's Intranet to determine that the entity's policies and procedures and employee handbook were made available to employees through the entity's Intranet.	No exceptions noted.
		Upon hire, employees are required to complete information security and awareness training.	Inspected the completed information security and awareness training certificate 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 completed information security and awareness training for a sample of current employees to determine that current employees were complete information security and awareness training on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook.	Inspected the signed employee handbook acknowledgment 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				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis.	No exceptions noted.
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected a summit meeting presentation 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.
		An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Inspected the anonymous reporting hotline to determine that an anonymous hotline was in place to allow employees, third-parties, and customers 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 Intranet.	Inspected the entity's Intranet to determine that changes to job roles and responsibilities were communicated to personnel through the entity's Intranet.	No exceptions noted.
		Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the entity's Intranet.	Inspected the incident response policies and procedures and the entity's Intranet to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and made available to employees through the entity's Intranet.	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 objectives, including changes made to the objectives, are communicated to its personnel through the entity's Intranet.	Inspected the entity's Intranet to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's Intranet.	No exceptions noted.
		Management tracks and monitors compliance with information security and awareness training requirements.	Inspected the information security and awareness training tracker to determine that management tracked and monitored compliance with information security and awareness training requirements.	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 master third-party agreement to determine that the entity's third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.
			Inspected the signed third-party agreement for a sample of third-parties to determine that the entity's third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		The entity's third-party agreement communicates the system commitments and requirements of third-parties.	Inspected the master third-party agreement to determine that the entity's third-party agreement communicated the system commitments and requirements of third-parties.	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 signed third-party agreement for a sample of third-parties to determine that the entity's third-party agreement communicated the system commitments and requirements of third-parties.	No exceptions noted.
		The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users prior to allowing them access to the system.	Inspected the entity's Intranet to determine that the information security policies and procedures that communicate the system commitments and requirements of external users were provided to external users prior to allowing them access to the system.	No exceptions noted.
		The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third-parties.	Inspected the master third-party agreement to determine that the entity's third-party agreement outlined and communicated the terms, conditions and responsibilities of third-parties.	No exceptions noted.
			Inspected the signed third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated the terms, conditions and responsibilities of third-parties.	No exceptions noted.
		The entity's contractor agreement outlines and communicates the terms, conditions and responsibilities of external users.	Inspected the master contractor agreement to determine that the entity's contractor agreement outlined and communicated the terms, conditions and responsibilities of external users.	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**
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the master customer agreement to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
			Inspected the signed customer agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
		Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties.	Inspected the incident response policies and procedures and the entity's Intranet to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and shared with external parties.	No exceptions noted.
		An anonymous hotline is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Inspected the anonymous reporting hotline to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	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 organizational chart, employee performance policies and procedures and the entity's documented objectives and strategies 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 entity's documented objectives and strategies to determine that executive management had documented objectives that were specific, measurable, attainable, relevant and time-bound (SMART).	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the risk assessment and management policies and procedures to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
			Inspected 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.

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**
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators for operational and internal controls effectiveness 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.
		The entity has defined the desired level of performance and operation in order to achieve the established entity objectives.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that the entity defined the desired level of performance and operation in order to achieve the established entity objectives.	No exceptions noted.
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the employee performance evaluation policies and procedures, the entity's documented objectives and strategies and the documented key performance indicators for operational and internal controls effectiveness to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies.	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**
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the entity's business plans, budget, and documented objectives and strategies 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 an annual basis.	Inspected the summit meeting presentation to determine that entity strategies, objectives and budgets were assessed on an annual basis.	No exceptions noted.
		The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures.	Inspected the completed internal controls matrix and the current registry of relevant regulatory, statutory, legislative and contractual 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 entity's documented objectives and strategies and the current registry of relevant regulatory, statutory, legislative and contractual 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.

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**
CC3.2	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 risk assessment and management policies and procedures 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 risk assessment and management policies and procedures 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 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				
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 risk assessment and management policies and procedures to determine that the entity's risk assessment process included: • 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	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 completed risk assessment to determine that the entity's risk assessment process included: • 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	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk assessment and management policies and procedures to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	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 completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures to determine that management developed risk mitigation strategies 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 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 risk assessment and management policies and procedures 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.

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 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.
		As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	Inspected the risk assessment and management policies and procedures to determine that as part of the annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	No exceptions noted.
			Inspected the completed risk assessment to determine that as part of the annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	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 fraud 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**
		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 fraud 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 fraud 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 fraud 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.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures 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.

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 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 risk assessment and management policies and procedures to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected 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 risk assessment and management policies and procedures 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.
			Inspected 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 rulesets for the production environments 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.
		Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.	Inspected the entity policies and procedures to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
		On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the internal management meeting invite and agenda to determine that on an annual basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.
		Control self-assessments that include logical access reviews and backup restoration tests are performed at least on an annual basis.	Inquired of the Chief Executive Officer regarding access reviews to determine that control self-assessments that included logical access reviews and backup restoration tests were performed at least 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 completed backup restoration test and the completed user access review to determine that control self-assessments that included logical access reviews and backup restoration tests were performed at least on an annual basis.	No exceptions noted.
		Vulnerability scans are performed weekly on the environment to identify control gaps and vulnerabilities.	Inspected the completed vulnerability scan results for a sample of weeks to determine that vulnerability scans were performed weekly on the environment to identify control gaps and vulnerabilities.	No exceptions noted.
		A third-party performs a 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 at least an annual basis.	Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on at least 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**
		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.	Inquired of the Chief Executive Officer regarding vendor and third-party management to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
			Inspected the completed review of the third-party attestation report for a sample of third-parties to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's 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.
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.	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 Chief Executive Officer regarding vulnerability management 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.

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 and the completed internal controls matrix 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 vulnerabilities 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 control gaps 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.
		Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are documented, investigated, and addressed.	Inquired of the Chief Executive Officer regarding vulnerability management to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance 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 and completed internal controls matrix to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of vulnerabilities to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of control gaps to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.
		Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are addressed by those parties responsible for taking corrective actions.	Inquired of the Chief Executive Officer regarding vulnerability management to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were addressed by 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 completed risk assessment and completed internal controls matrix to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of vulnerabilities to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of control gaps to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
		Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the internal management meeting invite and agenda to determine that management tracked whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed were addressed in a timely manner.	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.	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 Chief Executive Officer regarding vulnerability management 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 control gaps 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.

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 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.
		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 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.
		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.

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**
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures 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.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Organizational and information security policies and procedures are documented and made available to employee's through the entity's Intranet.	Inspected the organizational and information security policies and procedures and the entity's Intranet to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's Intranet.	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**
		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.
		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 is required for business operations • Authentication of access • Protecting the entity's assets from external threats	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.	Organizational and information security policies and procedures are documented and made available to employee's through the entity's Intranet.	Inspected the organizational and information security policies and procedures and the entity's Intranet to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's Intranet.	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**
		The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel.	Inspected the organizational and information security policies and procedures to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	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.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's Intranet.	Inspected the job description for a sample of job roles and the entity's Intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's Intranet.	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 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.

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 architectures over protected information assets to protect them from security events 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 policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
	Network (Microsoft 365)			
		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 user accounts accessible by authorized personnel.	Inquired of the Chief Executive Officer regarding administrative access to determine that network administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the network administrator user listing and access rights to determine that network administrative access was restricted to user accounts accessible by 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**
		Networks are configured to enforce password requirements that include: • Password age • Password length • Complexity • Multifactor authentication (MFA)	Inspected the network password settings to determine that networks were configured to enforce password requirements that included: • Password age • Password length • Complexity • MFA	No exceptions noted.
		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.	Inspected the network audit logging settings and an example network audit log extract to determine that network audit logging settings were in place.	No exceptions noted.
		Network audit logs are maintained and reviewed as needed.	Inquired of the Chief Executive Officer regarding audit logs to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected the network audit log settings and an example 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 (Linux)			
		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.
		Operating system administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Chief Executive Officer regarding administrative access to determine that operating system administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the operating system administrator user listing and access rights to determine that operating system administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Operating systems are configured to enforce secure shell (SSH) authentication configurations.	Inspected the operating system password settings to determine that operating systems were configured to enforce SSH authentication configurations.	No exceptions noted.
		Operating system account lockout settings are in place for account lockout threshold and duration.	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place for account lockout threshold and duration.	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 audit logging settings are in place.	Inspected the operating system audit logging settings and an example operating system audit log extract to determine that operating system audit logging settings were in place.	No exceptions noted.
		Operating system audit logs are maintained and reviewed as needed.	Inquired of the Chief Executive Officer regarding audit logs to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected the operating system audit log settings and an example operating system audit log extract to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
	Database (PostgreSQL)			
		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 user accounts accessible by authorized personnel.	Inquired of the Chief Executive Officer regarding administrative access to determine that database administrative access was restricted to user accounts accessible by 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**
			Inspected the database administrator user listing and access rights to determine that database administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Databases are configured to enforce password requirements.	Inspected the database password settings to determine that database were configured to enforce password requirements.	No exceptions noted.
		Database account lockout settings are in place.	Inspected the database account lockout settings to determine that database account lockout settings were in place.	No exceptions noted.
		Database audit logging settings are in place.	Inspected the database audit logging settings and an example database audit log extract to determine that database audit logging settings were in place.	No exceptions noted.
		Database audit logs are maintained and reviewed as needed.	Inquired of the Chief Executive Officer regarding audit logs to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected the database audit log settings and an example database audit log extract to determine that database 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**
	Application (Ruby on Rails)			
		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.
		Application administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the Chief Executive Officer regarding administrative access to determine that application administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the application administrator user listing and access rights to determine that application administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		The application is configured to enforce password requirements that include password length and complexity.	Inspected the application password settings to determine that application was configured to enforce password requirements that included password length and complexity.	No exceptions noted.
		Application account lockout settings are in place for lockout threshold and lockout duration.	Inspected the application account lockout settings to determine that application account lockout settings were in place for lockout threshold and lockout duration.	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 application is configured to log user actions and system events.	Inspected the audit logging code script within the application and an example application audit log extract to determine that application audit logging settings were in place.	No exceptions noted.
		Application audit logs are maintained and reviewed as needed.	Inquired of the Chief Executive Officer regarding audit logs to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected the audit logging code script within the application and an example application audit log extract to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
	Remote Access (Open VPN)			
		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.
		The ability to administer VPN access is restricted to user accounts accessible by authorized personnel.	Inquired of the Chief Executive Officer regarding administrative access to determine that the ability to administer VPN access was restricted to user accounts accessible by 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**
			Inspected the VPN administrator user listing to determine that the ability to administer VPN access was restricted to user accounts accessible by authorized personnel.	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.
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inspected the network diagram, firewall configurations and the demilitarized zone (DMZ) settings to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.
		Data coming into the environment is secured and monitored through the use of firewalls and an IPS.	Inspected the IPS configurations, firewall rulesets for the production environments 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 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 Transport Layer Security (TLS) encryption with a trusted certificate authority.	Inspected the 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 Advanced Encryption Standard (AES).	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES.	No exceptions noted.
		Logical access reviews are performed at least on an annual basis.	Inquired of the Chief Executive Officer regarding access reviews to determine that logical access reviews were performed at least on an annual basis.	No exceptions noted.
			Inspected the completed user access review to determine that logical access reviews were performed at least on an annual basis.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, the network, operating system, database, application, and VPN user listings, and the 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 for an employee as a component of the termination process.	Inspected the termination procedures, the network, operating system, database, application, and VPN user listings, and the 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 policies and procedures to determine that 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 hiring procedures, the network, operating system, database, application, and VPN user listings, and the 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 for an employee as a component of the termination process.	Inspected the termination procedures, the network, operating system, database, application, and VPN user listings, and the 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 at least on an annual basis.	Inquired of the Chief Executive Officer regarding access reviews to determine that logical access reviews were performed at least on an annual basis.	No exceptions noted.
			Inspected the completed user access review to determine that logical access reviews were performed at least on 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**
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 policies and procedures to determine that 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 hiring procedures, the network, operating system, database, application, and VPN user listings, and the 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 for an employee as a component of the termination process.	Inspected the termination procedures, the network, operating system, database, application, and VPN user listings, and the 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 at least on an annual basis.	Inquired of the Chief Executive Officer regarding access reviews to determine that logical access reviews were performed at least on 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**
			Inspected the completed user access review to determine that logical access reviews were performed at least on an annual basis.	No exceptions noted.
	Network (Microsoft 365)			
		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 (Linux)			
		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 (PostgreSQL)			
		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 (Ruby on Rails)			
		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 (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is 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 record retention and destruction policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		Data that is no longer required for business purposes is rendered unreadable.	Inquired of the Chief Executive Officer regarding data destruction to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the record retention and destruction policies and procedures to determine that 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 destruction certification for a sample of data destruction requests to determine that data that was no longer required for business purposes was rendered unreadable.	Testing of the control activity disclosed that there were no data destruction requests during the review period.
		Policies and procedures are in place for removal of media storing critical data or software.	Inspected the removable media policies and procedures to determine that policies and procedures were in place for removal of media storing critical data or software.	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 the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		VPN, TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN, TLS and other encryption technologies 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.

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 the 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.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and the digital certificate to determine that transmission of digital output beyond the boundary of the system 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.
		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				
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 firewall rulesets 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.
			Inspected the firewall rulesets 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 the 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 the IPS notification configurations, an IPS log extract, and an IPS alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	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**
		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 centralized antivirus software dashboard console and configurations to determine that centralized 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 centralized 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 continuous basis.	Inspected the centralized antivirus settings to determine that the antivirus software was configured to scan workstations on a continuous basis.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the AES.	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES.	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**
CC6.7	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 authorized personnel.	Inquired of the Chief Executive Officer regarding privileged access 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.
		The ability to recall backed up data is restricted to authorized personnel.	Inquired of the Chief Executive Officer regarding privileged access 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 recall backup media from the third-party storage facility to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
		The entity secures its environment using a multi-layered defense approach that includes firewalls, an IPS, antivirus software and a DMZ.	Inspected the network diagram, IPS configurations, firewall rulesets for the production environments, antivirus settings and DMZ settings to determine that the entity secured its environment using a multi-layered defense approach that included firewalls, an IPS, antivirus software and a DMZ.	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**
		VPN, TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN, TLS and other encryption technologies 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 the 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.
		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.
			Inspected the firewall rulesets 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				
Logical and Physical Access Controls				
CC6.0	**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.
			Inspected the firewall rulesets 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 the 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 the 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 the IPS notification configurations, an IPS log extract, and an IPS alert notification to determine that the IPS was configured to notify personnel upon intrusion prevention.	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**
		Critical data is stored in encrypted format using software supporting the AES.	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES.	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.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and the digital certificate to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		Mobile devices are protected through the use of secured, encrypted connections.	Inspected the encryption configurations for mobile devices to determine that mobile devices were protected through the use of secured, encrypted connections.	No exceptions noted.
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.	The ability to install applications and software is restricted to authorized personnel.	Inspected the denial notification received when an employee attempted to download an application or software to determine that the ability to install applications and software 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**
		FIM software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the 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 the FIM configurations and an example FIM notification log 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 centralized antivirus software dashboard console and configurations to determine that centralized 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 centralized 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				
Logical and Physical Access Controls				
CC6.0	**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 continuous basis.	Inspected the centralized antivirus settings to determine that the antivirus software was configured to scan workstations on a continuous 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**
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 policies and procedures 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 rulesets for the production environments 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, an example alert generated from the FIM software, an example log extract from the IPS and an example 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.

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 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 the IPS notification configurations, an IPS log extract, and an 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 the 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 the FIM configurations and an example FIM notification log 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 policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	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**
			Inspected the firewall rulesets 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.
			Inspected the firewall rulesets 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 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.
		Internal and external vulnerability scans and penetration tests are performed on at least an annual basis and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results for a sample of weeks and the completed penetration test results to determine that internal and external vulnerability scans and penetration tests were performed on at least an annual basis and remedial actions were taken where necessary.	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 and escalation 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 and escalation 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 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.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software, an example log extract from the IPS and an example IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	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**
		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 rulesets for the production environments 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.
		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 the 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 the IPS notification configurations, an IPS log extract, and an 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 the 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 the FIM configurations and an example FIM notification log 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.
			Inspected the firewall rulesets 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.
			Inspected the firewall rulesets 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.

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**
		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 centralized antivirus software dashboard console and configurations to determine that centralized 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 centralized 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 continuous basis.	Inspected the centralized antivirus settings to determine that the antivirus software was configured to scan workstations on a continuous basis.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
	Network (Microsoft 365)			
		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.

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 audit logging settings are in place.	Inspected the network audit logging settings and an example network audit log extract to determine that network audit logging settings were in place.	No exceptions noted.
		Network audit logs are maintained and reviewed as needed.	Inquired of the Chief Executive Officer regarding audit logs to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected the network audit log settings and an example network audit log extract to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
	Operating System (Linux)			
		Operating system account lockout settings are in place for account lockout threshold and duration.	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place for account lockout threshold and duration.	No exceptions noted.
		Operating system audit logging settings are in place.	Inspected the operating system audit logging settings and an example operating system audit log extract to determine that operating system audit logging settings were in place.	No exceptions noted.
		Operating system audit logs are maintained and reviewed as needed.	Inquired of the Chief Executive Officer regarding audit logs 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**
			Inspected the operating system audit log settings and an example operating system audit log extract to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
	Database (PostgreSQL)			
		Database account lockout settings are in place.	Inspected the VPN account lockout settings to determine that database account lockout settings were in place.	No exceptions noted.
		Database audit logging settings are in place.	Inspected the database audit logging settings and an example database audit log extract to determine that database audit logging settings were in place.	No exceptions noted.
		Database audit logs are maintained and reviewed as needed.	Inquired of the Chief Executive Officer regarding audit logs to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected the database audit log settings and an example database audit log extract to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.
	Application (Ruby on Rails)			
		Application account lockout settings are in place for lockout threshold and lockout duration.	Inspected the application account lockout settings to determine that application account lockout settings were in place for lockout threshold and lockout duration.	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 application is configured to log user actions and system events.	Inspected the audit logging code script within the application and an example application audit log extract to determine that application audit logging settings were in place.	No exceptions noted.
		Application audit logs are maintained and reviewed as needed.	Inquired of the Chief Executive Officer regarding audit logs to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected the audit logging code script within the application and an example application audit log extract to determine that application audit logs were maintained and reviewed as needed.	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.
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 and escalation 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 and escalation 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.

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 incident response and escalation 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 and escalation 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 Chief Executive Officer regarding incident resolution to determine that resolutions of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that resolutions of incidents were 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 resolutions of incidents were documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that no security incidents occurred during the review period.

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**
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Chief Executive Officer regarding incident resolution to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		Identified incidents are reviewed, monitored and investigated by an incident response team.	Inquired of the Chief Executive Officer regarding incident resolution to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	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 supporting incident ticket for a sample of incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		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 Chief Executive Officer regarding incident resolution to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine that 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 that 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 supporting incident ticket for a sample of incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine that the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Testing of the control activity disclosed that no security incidents occurred during the review period.
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.	Documented incident response and escalation 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 and escalation 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.	Inquired of the Chief Executive Officer regarding incident resolution to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

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 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.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inquired of the Chief Executive Officer regarding security incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		Documented incident response and escalation 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 and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents.	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**
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Chief Executive Officer regarding incident resolution to determine that resolutions of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that resolutions of incidents were 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 resolutions of incidents were documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.	Inquired of the Chief Executive Officer regarding security incidents to determine that remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that remediation actions taken for security incidents were 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 the supporting incident ticket for a sample of incidents to determine that the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		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 Chief Executive Officer 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.

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 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.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		The incident response and escalation 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 and escalation 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, and the system build guides 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 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 a semi-annual basis.	Inspected the completed backup restoration test to determine that backup restoration tests were performed on a semi-annual basis.	No exceptions noted.
		A business continuity and disaster recovery plan is 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.

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 disaster recovery plan is tested on an annual basis.	Inspected the completed disaster recovery test results to determine that the disaster recovery plan was tested on an annual basis.	No exceptions noted.
		The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results.	Inspected the business continuity and disaster recovery plans and completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plan and procedures were updated based on disaster recovery plan test results.	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.
		The change management process has defined the following roles and assignments: • Authorization of change requests - owner or business unit manager • Development - application design and support department • Testing - QA department • Implementation software change management group	Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests - owner or business unit manager • Development - application design and support department • Testing - QA department • Implementation software change management group	No exceptions noted.
		System changes are communicated to both affected internal and external users.	Inspected the update bulletin to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
		Access to implement changes in the production environment is restricted to authorized IT personnel.	Inquired of the Chief Executive Officer regarding administrative access to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	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 access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the supporting change ticket for a sample of application, network and system changes to determine that system changes were authorized and approved by management prior to implementation.	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.
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate development and production environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.
		System change requests are documented and tracked in a ticketing system.	Inspected the supporting change ticket for a sample of application, network and system changes to determine that system change requests were documented and tracked in a ticketing system.	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**
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	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 application, network and system changes to determine that system changes were tested prior to implementation, and that types of testing performed depended on the nature of the change.	No exceptions noted.
		Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.	Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools.	No exceptions noted.
		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.

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 risk assessment and management policies and procedures 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 risk assessment and management policies and procedures 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 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.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk assessment and management policies and procedures to determine that identified risks were rated using a risk evaluation process and ratings were approved 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**
			Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures to determine that management developed risk mitigation strategies 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 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 the 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.
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 risk assessment policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.	No exceptions noted.

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 develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the vendor risk assessment policies and procedures to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.
			Inspected the completed vendor risk assessment 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 rated using a risk evaluation process and ratings are approved by management.	Inspected the vendor risk assessment policies and procedures to determine that identified third-party risks were rated using a risk evaluation process and ratings are approved by management.	No exceptions noted.
			Inspected the completed vendor risk assessment to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	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 • Just cause for terminating the relationship	Inspected the master third-party agreement 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 signed third-party agreement for a sample of third-parties 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.	Inquired of the Chief Executive Officer regarding vendor and third-party management to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
			Inspected the completed review of the third-party attestation reports for a sample of third-parties to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's 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 the vendor risk assessment policies and procedures to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements.	No exceptions noted.