A-LIGN

Profisee Group, Inc.

Type 2 SOC 2 with HIPAA/HITECH

2024

Profisee

REPORT ON PROFISEE GROUP, INC.'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY WITH HIPAA/HITECH REQUIREMENTS

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

April 1, 2023 to January 31, 2024

Table of Contents

SECTION 1

ASSERTION OF PROFISEE GROUP, INC. MANAGEMENT

ASSERTION OF PROFISEE GROUP, INC. MANAGEMENT

February 26, 2024

We have prepared the accompanying description of Profisee Group, Inc.'s ('Profisee' or 'the Company') Database and File Management Software Services System titled "Profisee Group, Inc.'s Description of Its Database and File Management Software Services System throughout the period April 1, 2023 to January 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 Database and File Management Software Services System that may be useful when assessing the risks arising from interactions with Profisee Group, Inc.'s system, particularly information about system controls that Profisee Group, Inc. 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*) and essential elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009.

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

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

a. the description presents Profisee Group, Inc.'s Database and File Management Software Services System that was designed and implemented throughout the period April 1, 2023 to January 31, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period April 1, 2023 to January 31, 2024, to provide reasonable assurance that Profisee Group, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, 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 Profisee Group, Inc.'s controls throughout that period.

c. the controls stated in the description operated effectively throughout the period April 1, 2023 to January 31, 2024, to provide reasonable assurance that Profisee Group, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, if complementary subservice organization controls and complementary user entity controls assumed in the design of Profisee Group, Inc.'s controls operated effectively throughout that period.

Nick Powell
CFO
Profisee Group, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Profisee Group, Inc.

Scope

We have examined Profisee Group, Inc. accompanying description of its Database and File Management Software Services System titled "Profisee Group, Inc.'s Description of Its Database and File Management Software Services System throughout the period April 1, 2023 to January 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 April 1, 2023 to January 31, 2024, to provide reasonable assurance that Profisee Group, Inc.'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*). We have also examined the suitability of the design and operating effectiveness of controls to meet essential elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009.

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

The information included in section 5, "Other Information Provided by Profisee Group, Inc. Service Organization That Is Not Covered by the Service Auditor's Report," is presented by Profisee Group, Inc. management to provide additional information and is not a part of the description. Information about Profisee Group, Inc.'s management's response to testing exceptions has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Profisee Group, Inc.'s service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements.

Service Organization's Responsibilities

Profisee Group, Inc. 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 Profisee Group, Inc.'s service commitments and system requirements were achieved. Profisee Group, Inc. has provided the accompanying assertion titled "Assertion of Profisee Group, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Profisee Group, Inc. 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 HIPAA/HITECH requirements, 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 and HIPAA/HITECH requirements. 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 and HIPAA/HITECH requirements
- 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 and HIPAA/HITECH requirements
- 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 and HIPAA/HITECH requirements. 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 Profisee Group, Inc.'s Database and File Management Software Services System that was designed and implemented throughout the period April 1, 2023 to January 31, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period April 1, 2023 to January 31, 2024, to provide reasonable assurance that Profisee Group, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, 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 Profisee Group, Inc.'s controls throughout that period.
c. the controls stated in the description operated effectively throughout the period April 1, 2023 to January 31, 2024, to provide reasonable assurance that Profisee Group, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, if complementary subservice organization controls and complementary user entity controls assumed in the design of Profisee Group, Inc.'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 Profisee Group, Inc., user entities of Profisee Group, Inc.'s Database and File Management Software Services System during some or all of the period April 1, 2023 to January 31, 2024, business partners of Profisee Group, Inc. subject to risks arising from interactions with the Database and File Management 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 and HIPAA/HITECH requirements
- 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
February 26, 2024

SECTION 3

PROFISEE GROUP, INC.'S DESCRIPTION OF ITS DATABASE AND FILE MANAGEMENT SOFTWARE SERVICES SYSTEM THROUGHOUT THE PERIOD APRIL 1, 2023 TO JANUARY 31, 2024

OVERVIEW OF OPERATIONS

Company Background

Founded in 2007 and headquartered in Atlanta, Georgia, Profisee is a leading global provider of cloud native Master Data Management (MDM) software. Profisee's MDM solution helps organizations realize the full potential of their data by unifying data from disparate systems, enhancing incomplete information, correcting duplicate or incorrect records, and continually harmonizing data across data silos, creating a trusted foundation of a company's most critical information. Profisee is grounded and guided by its purpose; to make Master Data Management easy to unlock the power of trusted data. Customers can leverage Profisee MDM SaaS for a true Software-as-a-Service experience, or maintain complete deployment flexibility in any cloud, on-premise or via a hybrid model. With a low total cost of ownership, the fastest time to value in the industry, and a truly flexible multidomain platform, Profisee has quickly become the gold standard for master data management.

Description of Services Provided

Profisee provides Database and File Management Software services and the Profisee Application to allow for companies to query databases and systems that may otherwise be unable to integrate, update records across these systems and validate data with reputable sources. Profisee additionally allows for data science to evaluate inputs from these systems and data analytics to be applied across unintegrated systems and sources.

Principal Service Commitments and System Requirements

Profisee designs its systems and approach to the product to require as little interaction with outside systems as possible, reducing system exposure and protecting information systems as best as possible. Profisee's traditional deployment in PaaS and IaaS deployments require no interaction with Profisee Corporate systems to operate, no data is collected or processed by Profisee Corporate with this approach extending to our SaaS offering where applicable.

Profisee strives to be able to provide the best Master Data Management service with the least interaction from Profisee where possible, this includes limiting exposure of any information to unapproved users, meeting compliance requirements, following government regulatory standards, and establishing repeatable process where customers retain control and access to data without requiring approval for new access to be approved.

Profisee has committed to Service Level Agreements (SLA) with SaaS customers, where security commitments, availability of the platform and access control are used to design a service that is able to grow and expand while maintaining agreed upon SLAs.

Profisee has also integrated Terraform, Infrastructure as Code, to be able to ensure environments are deployed uniformly for each customer and reduce the likelihood of misconfigurations to be introduced, reducing the need of effort to ensure proper deployment and allow for the allocation of resources to be dedicated to design more secure environments.

Components of the System

Infrastructure

Primary infrastructure used to provide the Database and File Management Software Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Application Firewall	Azure	Provide filtering services for SaaS deployment
Jumpbox Virtual Machines (VM)		Control access to the SaaS environment
Kubernetes Services		Host and process requests for SaaS customers
SQL Servers		Host data for SaaS customers

Software

Primary software used to provide the Database and File Management Software Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Failover Region Pairs	Azure	Provide High Availability and recovery environments
Backup		Provide Long term recovery for customers
Defender		Perform antivirus scans, remediation activity and security monitoring services across Azure native systems where the Profisee SaaS solution is hosted
Azure Active Directory (AD)		Provides authentication and Single Sign-On (SSO) services for the SaaS solution. Profisee utilizes Azure AD for the users to authenticate, and customers integrate their Azure AD for SSO access to the Profisee SaaS solution

People

Profisee has approximately 140 employees organized in the following functional areas:

- **Corporate** - Executive team members are responsible for the delivery of various functions such as the development of the platform, sale of the products and review overall objectives and goals that the company has set.
- **Operations** - SaaS Operations teams is made of up individuals who are tasked with the operation, delivery, and monitoring of the SaaS solution. These team members support, troubleshoot and respond to tickets raised by customers. Information Technology (IT) Operations team is responsible for the operation, maintenance and administration of any device, IT service, hardware, software, or network service.
- **Sales** - Sales team is responsible for providing demonstration of the product, working with prospective customers, answers questions and any other activity during the sales process.

- **Professional Services** - Professional Services members are responsible for providing troubleshooting, aiding in the deployment of Profisee and resolving issues a customers may have in Traditional Deployments and SaaS deployments. These activities are conducted in either an "Over the Shoulder" manner where the customer is responsible for conducting the activity under the supervision of a Professional Services team member or with the guiding principle of Least Privilege where access to information or systems is granted on a need basis.
- **Marketing** - Marketing is responsible for the development of marketing material, slogans, tag lines and other related documents. Marketing also conducts research and education activities designed to better position Profisee in the MDM marketplace and ensure potential customers understand the value of the services provided.

Data

Data that is uploaded to the Profisee SaaS solution is at the discretion of the customer who retains ultimate access and authority of data that is stored. Profisee does not access or view customer data and enables Row Level Security is a default behavior to prevent unauthorized access. Profisee SaaS processes and stores any data that a customer uploads, data destruction is provided through Azure controls with confirmation able to be provided.

Because Profisee does not have insight into customer data, all data is treated with equal protection, all systems are covered by the same security controls, encryption at rest and in transit is enforced through all portions of the environment, and access must be approved by a customer and is controlled through a customer's Azure AD to ensure access control is provided.

Processes, Policies and Procedures

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

Physical Security

The in-scope system and supporting infrastructure is hosted by Azure. As such, Azure is responsible for the physical security controls for the in-scope system. Access is controlled through Azure VM Jump boxes to provide access control that are controlled through the same protections as all Azure systems with the availability agnostic to where an employee may be connecting from.

Logical Access

Profisee uses role-based access control, administered through Azure Active Directory, Azure AD Groups and Azure Roles to provide levels of access and control that can be granularly administered. Additionally logical access is controlled through the use of Jump Boxes and Virtual Private Network (VPN) isolation that is controlled through both logical access and AD group restrictions.

Profisee controls access through approved users requiring requesting access from appropriate parties, approval and requests be relevant to their job function. Customer access is controlled through customer's own processes and able to be determined by customer's unique controls and requirements.

Access records are recorded and logged in a central Security information and event management (SIEM) solution with controls to monitor for access modification activity, complex password requirements for access with a minimum character length of 12 characters, lockout events triggered after 5 failures that require manual investigation to unlock and time outs set for 5 minutes of inactivity.

All access is also required to satisfy Microsoft Azure AD Multi-factor Authentication (MFA) requests, with access revoked at the time of termination through the disabling and removal of the user AD account.

Customer access is controlled through a thick client connection to a customer's tenant in the Profisee SaaS solution, with Azure AD SSO used to approve authentication, using the customer's Azure AD. Traffic is encrypted with Transport Layer Security (TLS) 1.2 in transit and Application Programming Interface (API) access is limited to approved processes and sources.

Profisee reviews access on an annual basis for Profisee Employees to ensure only approved users and access for those users.

Computer Operations - Backups

Profisee utilizes Replication zones across region pairs in the region that is relevant, in the US this is East US and Central US. Profisee also offers up to 89 days of backups through the Azure Backup process in addition to the full replication from East US to Central US, or other region pairs.

Should a failover event need triggered, Profisee is able to manually trigger a fail over, and during annual testing we average 15 minutes for a full fail over, with partial operational functions within minutes.

Computer Operations - Availability

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

Profisee centrally logs security relevant information with Log Analytics and Azure Sentinel to provide monitoring of events, review logs and manage incidents.

Infrastructure is designed to run on Kubernetes which enables scalability as part of the design, which is also built on Azure Cloud allowing for scalability of the platform and resources. Profisee utilizes Azure to enable industry leading services that allow for infrastructure that is easy to patch, manage, increase capacity, backup strategy, storage and controls that are native. Profisee closely monitors open-source software and utilizes static code analysis for minor releases with an Application Penetration Assessment prior to any major releases.

Change Control

Profisee Change Control is currently tracked through Azure DevOps, with User Acceptance Testing (UAT) results are documented and maintained results that are required prior to promotion to Production. Changes to the Production environment require communication with any affected customer, backout plans, and approved service windows. Profisee conducts updates of the Profisee Platform as versions are released with any patching that can be automated through Azure systems being enabled.

Data Communications

Profisee utilizes Azure network controls including Application Firewall, Azure VPN and Azure Intrusion Detection and Prevention System (IPDS). Firewalls control Network Address Translation functionality to manage network exposure, with access to the firewalls restricted to approved users, policies applied by and controlled through Terraform to ensure uniformity between environments.

Profisee utilizes full redundancy provided through Azure to prevent any issue that would prevent operation at one data center from preventing service from ceasing and allowing for failover to happen, for example from East US to Central US.

Profisee has engaged Evolve Security to provide Application Pentest Assessment activities. Upon disclosure vulnerabilities are reviewed by Profisee, identified for priority and patched or remediated within time frame requirements based on severity. Malicious activity impact has been discussed and planned for, limiting all access to customer data from all employees, preventing unauthorized access or disclosure. Profisee has additionally engaged Horizon3 AI to provide Internal and External penetration testing services to discover vulnerabilities, misconfigurations and emerging cyber threats.

Approved users must access systems through Azure Jump Boxes, which require authentication, MFA requests and be an approved user of the jump box. Identity Access Control is then used to limit a user's access from the jump box to approved systems, following the least privilege access to grant access to the least required systems.

Boundaries of the System

The scope of this report includes the Database and File Management Software Services System performed in the Alpharetta, Georgia facilities.

This report does not include the cloud hosting services provided by Azure at various facilities.

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

Control Environment

Integrity and Ethical Values

Profisee's commitment to providing ethical administration of the SaaS solution have led to the design, functions and access controls of the Profisee Solution. As part of the employee on-boarding process Profisee's commitment to ethical behavior is a required training meeting that covers both the employee handbook as well as the Growth Mindset which is discussed during ongoing communications, employee celebrations and lessons learned activities where the Growth Mindset is used to frame lessons learned.

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

As part of the evaluation of employees and creation of the role descriptions competencies, certifications, and specific skills are identified and assessed for. Profisee also evaluates employees for alignment with the Growth Mindset as part of the evaluation phase.

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

Profisee'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. This can be most seen in Profisee collecting and accessing no customer data or selling information to 3rd parties in any manner.

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 with specific design decisions such as hosting in region to provide regulatory compliance.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

Profisee'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.

Relevant responsibilities and activities are assigned to individuals and teams best able to achieve the stated goals of the organization. These goals and strategies are laid out for all employees during an annual meeting that all employees are invited to attend.

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 and accessible through the Human Resources (HR) portal.

Human Resources Policies and Practices

Profisee's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Profisee'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 an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.
- To make the termination process, Profisee implements SSO and Identity based authentication in all possible solutions.

Risk Assessment Process

Profisee's risk assessment process identifies and manages risks that could potentially affect Profisee's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Profisee 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 Profisee, 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

Profisee reviews, updates, and identifies emerging threats on an annual basis, tracking these organizational risks with a central risk register, taking into consideration the likelihood of this risk occurring, the impact of the risk to the organization and system or information impacted by the risk. This report is used to plan for remediation efforts, plan for new controls and implement new and emerging technologies to reduce these risks.

Information and Communications Systems

Profisee establishes standard communication channels, stakeholders, and other relevant operational systems to communicate with customers and notify of changes, events, or receive feedback and suggestions.

Internal communications are provided at annual Town Halls, sprint reviews and other meetings to cover goals, strategy accomplishments and lessons learned with internal employees. E-mail communications are also sent to companywide mailing lists providing updates, information, and requests to all employees at an ad-hoc basis.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Profisee'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. Certification and renewal activities are used to monitor specific systems and controls are functioning, with feedback collected and used to strengthen existing controls, create new controls, and resolve any gaps that are identified during engagements.

Management's close involvement in Profisee'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.

Reporting Deficiencies

Management's close involvement in Profisee'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.

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Periodic Assessments

Profisee has a risk assessment process in place to identify and manage the risks that could affect the Company's ability to provide services to its user entities. The risk assessment procedure defines the responsibility, methodologies and processes used by Profisee to assess the risks while providing services and develop mitigation strategies to address those risks. This process requires the Company to identify risk based on management's internal knowledge of its operations. The following risk factors are discussed among the executive management including the Chief Executive Officer (CEO), Chief Technology Officer (CTO) and the Director of Client Services at periodic intervals:

- *Risk Assessment:* The risk assessment is performed by the risk management personnel. Risk factors associated with the delivery or implementation of services to customers are evaluated considering process owners, dependencies, timelines, and quality.
- *Health Information Security Risks:* Health information security risks are assessed by the Director of Information Services. Risk factors associated with the organization are evaluated considering compliance obligations, laws and regulations, policies and procedures, contracts, and best practices to which the organization has committed to. Information security assessments carried out by risk management personnel are rolled up to the CEO and the CTO of the organization.

Policies and Procedures

Health information security policies and procedures have been implemented regarding the protection of information assets. The policies and procedures act as a guide for all Profisee personnel. These policies and procedures define guidelines for the health information security program related to scope of services, which includes implementing and managing logical access security and controls, including the following:

- Health information security policy
- Asset management
- Data classification
- Business continuity
- Incident management
- Access control
- Physical security

These policies are reviewed and approved by management on at least an annual basis.

Security Awareness Training

Profisee employees receive security awareness training for health information security as part of the onboarding process. This training is reinforced by security awareness communications on current issues which are distributed annually. Additionally, employees are also required to participate in annual security awareness training.

Periodic Testing and Evaluation

Profisee completes evaluations throughout each calendar year regarding the effectiveness of the health information security program that include, but are not limited to, the following:

- Internal risk assessments
- Corrective action plans
- Management reviews

Remediation and Continuous Improvement

Areas of non-compliance in Profisee's internal control system surface from many sources, including the Company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings, if identified, of internal control non-compliant items should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to areas of non-compliance in internal control procedures and make the decision for addressing any non-compliant items based on whether the incident was isolated or requires a change in the Company's procedures or personnel.

Incident Response

Profisee maintains a documented incident response plan including breach notification requirements as mandated by HITECH. The procedures include, but are not limited to, the identification, response, escalation, and remediation of security breaches and other incidents. A formal breach notification process is utilized to document and track resolution of incidents noted. The incident response procedures are tested during the normal course of business and are updated as needed.

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.

Trust Services Criteria and HIPAA/HITECH Requirements Not Applicable to the System

The following Trust Services Criteria and HIPAA / HITECH requirements are not applicable to the system:

Trust Services Criteria and HIPAA / HITECH Requirements Not Applicable to the System		
Category / Safeguard	**Criteria / Requirement**	**Reason**
Administrative Safeguard	164.308(a)(4)(ii)(A)	The entity is not a healthcare clearinghouse.
	164.308(b)(1)	The entity is not a covered entity.
Organizational Requirement	164.314(a)(2)(ii)	The entity is not a government entity.
	164.314(b)(1)	The entity is not a plan sponsor.
	164.314(b)(2)	The entity is not a group health plan.
Physical Safeguard	164.310(c)	The entity is not a covered entity.

Trust Services Criteria and HIPAA / HITECH Requirements Not Applicable to the System		
Category / Safeguard	**Criteria / Requirement**	**Reason**
Breach Notification	164.404(a), 164.404(2), 164.404(b), 164.404(c)(1), 164.404(c)(2), 164.404(d)(1)(i), 164.404(d)(1)(ii), 164.404(d)(2), 164.404(d)(2)(i), 164.404(d)(2)(ii), 164.404(d)(3), 164.406, 164.408(a), 164.408(b), 164.408(c)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

Subservice Organizations

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

Subservice Description of Services

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

Complementary Subservice Organization Controls

Profisee'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 and HIPAA/HITECH requirements related to Profisee's services to be solely achieved by Profisee control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Profisee.

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

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.1, CC6.3, CC6.6	Access to the underlying network, virtualization management, and storage devices for its cloud hosting services where certain instances of the application reside is restricted to authorized personnel.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
	CC6.4, CC7.2, 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii)	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
	164.310(a)(2)(iv)	Policies and procedures are in place to document repairs and modifications to the physical components of the data center facility.
	164.310(d)(1), 164.310(d)(2)(iii)	Offsite backups are tracked and managed to maintain accuracy of the inventory information.
		Production data is encrypted on backup media.

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

- Reviewing and reconciling output reports
- Holding discussions with vendors and subservice organization
- Making regular site visits to vendor and subservice organization's facilities
- 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

Profisee'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 Profisee's services to be solely achieved by Profisee control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Profisee'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 organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Profisee.
2. User organizations should practice removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Profisee's services.
3. Transactions for user organizations relating to Profisee's services should be appropriately authorized, and transactions should be secure, timely, and complete.
4. For user organizations sending data to Profisee, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.
5. User organizations should implement controls requiring additional approval procedures for critical transactions relating to Profisee's services.
6. User organizations should report to Profisee in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Profisee.
7. User organizations are responsible for notifying Profisee in a timely manner of any changes to personnel directly involved with services performed by Profisee. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by Profisee.
8. User organizations are responsible for adhering to the terms and conditions stated within their contracts with Profisee.
9. User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by Profisee.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Criteria

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.

HEALTH INFORMATION SECURITY PROGRAM

Profisee has developed a health information security management program to meet the information security and compliance requirements related to Artificial Intelligence and Natural Language Processing services and its customer base. The program incorporates the elements of the HIPAA and the HITECH. The description below is a summary of safeguards that Profisee has implemented to adhere to the applicable components of HIPAA Final Security Rule and the breach notification requirements of HITECH.

Administrative Safeguards - Policies and procedures designed to show Profisee complies with the act:

- Management has adopted a written set of health information security policies and designated the information security officer to be responsible for developing and implementing the required policies and procedures.
- Procedures address access authorization, establishment, modification, and termination.
- Documented incident response policies for reporting security incidents are in place to guide employees in identifying, reporting, of security incidents.
- Business continuity plans are documented to enable continuation of critical business processes in the event of an emergency.
- Privileged administrative access to systems is restricted to authorized individuals.
- Automated backup systems are in place to perform scheduled replication of production data and systems at pre-defined intervals.
- Antivirus software is utilized to detect and eliminate data or files that contain certain virus signatures on certain production servers.

Physical Safeguards - Controlling physical access to protected data:

- Documented physical security policies and procedures are in place to guide personnel in physical security administration.
- Physical access procedures are in place restrict access, log visitors, and terminate access to the office facility.
- Inventory listings are utilized to track and monitor hardware and removable media.
- Data destruction procedures are in place to guide the secure disposal of data and media.

Technical Safeguards - Controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient:

- Access to in-scope systems is restricted to authorized personnel based on a valid user account and password.
- Systems are configured to enforce pre-determined thresholds to lock user sessions due to invalid login attempts.
- Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.

Organizational Requirements - Adherence to policies and procedures in regard to PHI documentation availability, as well as documentation retention:

- Documented policies address the confidentiality threshold of PHI documents and the length of time they should be retained before being destroyed.
- Contractual responsibilities by subparts of an organization are written and maintained in contracts.
- Separation of duties is existent in order to protect to confidentiality, availability, and integrity of PHI.
- Ensure that only appropriate parties gain access to PHI internally and external to the organization.

Breach Notification - A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach:

- Documented policies and procedures are in place to guide personnel in notifying the covered entity upon discovery of a breach.
- Documented policies and procedures are in place to guide personnel in responding to discovery of a breach.

- Documented policies and procedures require disclosure of the unsecured protected health information and include, to the extent possible, the identification of each individual and a description of the event.
- Documented policies and procedures are in place to guide personnel in the exception processes of delaying and documenting notifications.
- Documented policies and procedures are in place to guide personnel in documentation of administrative requirements for demonstrating that all notifications were made as required.

Control Activities Specified by the Service Organization

The applicable trust criteria and HIPAA/HITECH requirements, 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 criteria and HIPAA/HITECH requirements and related control activities are included in Section 4, they are, nevertheless, an integral part of Profisee's description of the system. Any applicable trust services criteria or HIPAA/HITECH requirements that are not addressed by control activities at Profisee are described within Section 4 and within the Subservice Organization and Criteria Not Applicable to the System sections above.

SECTION 4

TRUST SERVICES CATEGORY, CRITERIA, HIPAA/HITECH REQUIREMENTS, RELATED CONTROLS, AND TESTS OF CONTROLS

GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, HIPAA/HITECH REQUIREMENTS, RELATED CONTROLS, AND TESTS OF CONTROLS

A-LIGN ASSURANCE's examination of the controls of Profisee was limited to the Trust Services Criteria and HIPAA/HITECH requirements, related criteria and control activities specified by the management of Profisee and did not encompass all aspects of Profisee'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 aspects of the service organization's controls that may affect the HIPAA/HITECH requirements
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization
- Understand the flow of ePHI through the service organization
- Determine whether the criteria are relevant to the user entity's assertions
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria
- Determine whether the service organization's controls are suitably designed to meet the health information security program of the user entity's and determine whether they have been implemented

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, procedures, the code of conduct and the employee handbook.	Inspected the employee handbook and the entity's SharePoint site to determine that core values were communicated from executive management to personnel through policies, procedures, the code of conduct 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.
		Prior to hire, personnel are required to acknowledge the employee handbook.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that prior to hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.
		Prior to hire, personnel are required to complete a background check.	Inquired of the Talent Acquisition Consultant regarding the background checks for new hires and determined that prior to hire, personnel were required to complete a background check.	No exceptions noted.
			Observed the completed background check for a sample of new hires and determined that prior to 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**
			Inspected the employee handbook to determine that prior to hire, personnel were required to complete a background check.	No exceptions noted.
		Prior to hire, personnel are required to sign a confidentiality agreement.	Inspected the signed confidentiality agreement for a sample of new hires to determine that prior to hire, personnel were required to sign a confidentiality agreement.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct when changes are made.	Inquired of the Senior Security Engineer regarding the employee handbook acknowledgement to determine that personnel were required to acknowledge the employee handbook and code of conduct when changes were made.	No exceptions noted.
			Inspected the employee handbook to determine that personnel were required to acknowledge the employee handbook and code of conduct when changes were made.	No exceptions noted.
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct when changes were made.	Testing of the control activity disclosed that there were no changes made to the employee handbook that required employee acknowledgement during the review period.

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.
		Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the sanction policies within the employee handbook to determine that sanction policies, which included probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.
		Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inquired of the Senior Security Engineer regarding how employees and third parties report unethical behavior to determine that employees, third parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
			Inspected the entity's SharePoint and support site to determine that employees, third parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
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 defines and documents the skills and expertise needed among its members.	Inspected the executive management job descriptions for a sample of executive management job roles to determine that executive management defined and documented the skills and expertise needed among its members.	No exceptions noted.
		Executive management roles and responsibilities are documented and reviewed as needed.	Inquired of the Senior Security Engineer regarding the executive management job role revision to determine that executive management roles and responsibilities were documented and reviewed as needed.	No exceptions noted.
			Inspected the executive management job descriptions for a sample of executive management job roles to determine that executive management roles and responsibilities were documented and reviewed as needed.	No exceptions noted.
		Executive management evaluates the skills and expertise of its members annually.	Inquired of the Senior Security Engineer regarding the executive management evaluations to determine that executive management evaluated the skills and expertise of its members annually.	No exceptions noted.
			Inspected the employee handbook to determine that executive management evaluated the skills and expertise of its members annually.	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 performance evaluation form for a sample of executive management members to determine that executive management evaluated the skills and expertise of its members annually.	Testing of the control activity disclosed that a performance evaluation for one executive management member sampled was not documented. Inquired with the Senior Security Engineer regarding the executive management performance evaluation and determined the executive management member had a daily meeting repurposed to conduct this activity.
		Executive management maintains independence from those that operate the key controls within the environment.	Inspected the organizational chart and internal controls matrix to determine that executive management maintained independence from those that operated the key controls within the environment.	No exceptions noted.
		Executive management meets at least annually with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected the Cybersecurity Tabletop meeting slide deck, notes, and meeting invite to determine that executive management met at least 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**
		Executive management evaluates the skills and competencies of those that operate the internal controls within the environment annually.	Inspected the completed performance and conduct evaluation form for a sample of current employees to determine that executive management evaluated the skills and competencies of those that operate the internal controls within the environment annually.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the internal controls matrix and the weekly security review meeting invite 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 at least annually and makes updates to the organizational structure and lines of reporting, if necessary.	Inquired of the Senior Security Engineer regarding the revision history of the organizational chart to determine that executive management reviewed the organizational chart at least annually and made updates to the organizational structure and lines of reporting, if necessary.	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 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 SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Executive management reviews job descriptions as needed and makes updates, if necessary.	Inspected the job description including the revision date for a sample of job roles to determine that executive management reviewed job descriptions as needed and made updates, if necessary.	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 internal controls matrix, and the job description for a sample of job roles to determine that executive management had established proper segregations of duties for key job functions and roles within the organization.	No exceptions noted.

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**
		Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system.	Inspected the job description for a sample of job roles to determine that roles and responsibilities defined in written job descriptions considered and addressed specific requirements relevant to the system.	No exceptions noted.
		A vendor risk assessment is performed on at least an annual basis which includes reviewing the activities performed by third parties.	Inspected the vendor risk management policies and procedures to determine that a vendor risk assessment was performed on at least an annual basis which included reviewing the activities performed by third parties.	No exceptions noted.
			Inspected the risk assessment inclusive of vendor risks to determine that a vendor risk assessment was performed on at least an annual basis which included reviewing the activities performed by third parties.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee handbook and the security governance policy to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.

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**
		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 employee handbook and the job opening postings on the entity's website 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.
		The entity evaluates the competencies and experience of candidates prior to hiring.	Inspected the candidate 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.
		The entity evaluates the competencies and experience of third parties prior to working with them.	Inquired of the Senior Security Engineer regarding the third-party evaluation process to determine that the entity evaluated the competencies and experience of third parties prior to working with them.	No exceptions noted.
			Inspected the vendor risk management policy to determine that the entity evaluated the competencies and experience of third parties prior to working with them.	No exceptions noted.
			Inspected the third-party review meeting invite for a sample of third parties to determine that the entity evaluated the competencies and experience of third parties prior to working with them.	Testing of the control activity disclosed that the entity did not evaluate the competencies and experience for one of three third parties sampled.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.	Inspected the job description for a sample of job roles and the candidate 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 were evaluated as part of the hiring process.	No exceptions noted.
		Prior to hire, personnel are required to complete a background check.	Inquired of the Talent Acquisition Consultant regarding the background checks for new hires and determined that prior to hire, personnel were required to complete a background check.	No exceptions noted.
			Observed the completed background check for a sample of new hires and determined that prior to hire, personnel were required to complete a background check.	No exceptions noted.
			Inspected the employee handbook to determine that prior to hire, personnel were required to complete a background check.	No exceptions noted.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the professional development training catalog to determine that employees were required to attend continued training annually that related 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 training completion dashboard 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 tracks and monitors compliance with continued professional education (CPE) training requirements.	Inspected the professional development training catalog to determine that executive management tracked and monitored compliance with CPE training requirements.	No exceptions noted.
		Executive management uses an outside vendor to assist with its continued training of employees.	Inspected the third-party agreement to determine that executive management used an outside vendor to assist with its continued training of employees.	No exceptions noted.
		Upon hire, personnel are required to complete information security awareness training.	Inspected the information security awareness training onboarding meeting invite for a sample of new hires to determine that upon hire, personnel were required to complete information security awareness training.	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 handbook to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations as it related 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**
		The entity assesses training needs on an annual basis.	Inspected the professional development training catalog slide deck to determine that the entity assessed training needs on an annual basis.	No exceptions noted.
		As part of the entity's contingency plan for job roles and assignments important to the operations and performance of controls, the entity cross trains its personnel.	Inspected the training program materials to determine that as part of the entity's contingency plan for job roles and assignments important to the operations and performance of controls, the entity cross trained its personnel.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Prior to hire, personnel are required to acknowledge the employee handbook.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that prior to hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are required to acknowledge the employee handbook and code of conduct when changes are made.	Inquired of the Senior Security Engineer regarding the employee handbook acknowledgement to determine that personnel were required to acknowledge the employee handbook and code of conduct when changes were made.	No exceptions noted.
			Inspected the employee handbook to determine that personnel were required to acknowledge the employee handbook and code of conduct when changes were made.	No exceptions noted.
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct when changes were made.	Testing of the control activity disclosed that there were no changes made to the employee handbook that required employee acknowledgement during the review period.
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee handbook and the security governance policy to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management has established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities.	Inspected the employee handbook 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 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 an annual basis.	No exceptions noted.
		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 handbook 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 did not meet expectations as it related to their job role and responsibilities.	No exceptions noted.
		Executive management reviews the job requirements and responsibilities documented within job descriptions as needed and makes updates, if necessary.	Inspected the job description including the revision date for a sample of job roles to determine that executive management reviewed the job requirements and responsibilities documented within job descriptions as needed and made updates, if necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the sanction policies within the employee handbook to determine that sanction policies, which included probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inquired of the Senior Security Engineer regarding the edit checks to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
			Observed the input of information into the in-scope system to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
			Inspected the system edit check configurations to determine that edits checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
		Architecture diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the architecture diagram to determine that architecture diagrams were 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 entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the change detection and monitoring software configurations, the intrusion detection and prevention system (IDPS) configurations, the encryption methods, and configurations for data at rest and in transit, and the virtual private network (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 entered into the system is captured correctly.	Inquired of the Senior Security Engineer regarding the edit checks to determine that data entered into the system was captured correctly.	No exceptions noted.
			Observed the input of information into the in-scope system to determine that data entered into the system was captured correctly.	No exceptions noted.
			Inspected the system edit check configurations to determine that data entered into the system was captured correctly.	No exceptions noted.
		Data processed within the system is reviewed for completeness and accuracy annually.	Inquired of the Senior Security Engineer regarding the data completeness and accuracy review to determine that data processed within the system was reviewed for completeness and accuracy annually.	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 data classification policy to determine that data processed within the system was reviewed for completeness and accuracy annually.	No exceptions noted.
			Inspected the data review management reports to determine that data processed within the system was reviewed for completeness and accuracy annually.	Testing of the control activity disclosed that no data review management reports were made during the review period. Inquired with the Senior Security Engineer regarding the data completeness and accuracy review and determined that the data reviews were made upon customer request.
		Data output from the system is reviewed for completeness and accuracy annually.	Inquired of the Senior Security Engineer regarding the data completeness and accuracy review to determine that data output from the system was reviewed for completeness and accuracy annually.	No exceptions noted.
			Inspected the data classification policy to determine that data output from the system was reviewed for completeness and accuracy annually.	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 data review management reports to determine that data output from the system was reviewed for completeness and accuracy annually.	Testing of the control activity disclosed that no data review management reports were made during the review period. Inquired with the Senior Security Engineer regarding the data completeness and accuracy review and determined that the data reviews were made upon customer request.
		Data and information critical to the system are assessed annually for relevance and use.	Inspected the data classification policies and procedures to determine that data and information critical to the system were 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 Senior Security Engineer regarding data retention 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 data classification and secure disposal 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.

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.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		The entity's policies and procedures, code of conduct and employee handbook are made available to personnel through the entity's SharePoint site.	Inquired of the Senior Security Engineer regarding the entity's SharePoint site to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to personnel through the entity's SharePoint site.	No exceptions noted.
			Observed the entity's SharePoint site to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to personnel through the entity's SharePoint site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the entity's SharePoint site to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to personnel through the entity's SharePoint site.	No exceptions noted.
		Upon hire, personnel are required to read and acknowledge the employe handbook which contain information security policies and procedures.	Inspected the signed employee handbook for a sample of new hires to determine that upon hire, personnel were required to read and acknowledge the employe handbook which contain information security policies and procedures.	No exceptions noted.
		Upon hire, personnel are required to complete information security awareness training.	Inspected the information security awareness training onboarding meeting invite for a sample of new hires to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
		Current employees are required to read and acknowledge the employee handbook when changes are made.	Inquired of the Senior Security Engineer regarding the employee handbook acknowledgement to determine that current employees were required to read and acknowledge the employee handbook when changes were made.	No exceptions noted.
			Inspected the employe handbook to determine that current employees were required to read and acknowledge the employee handbook when changes were made.	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 employee handbook and code of conduct acknowledgement for a sample of current employees to determine that current employees were required to read and acknowledge the employee handbook when changes were made.	Testing of the control activity disclosed that there were no changes made to the employee handbook that required employee acknowledgement during the review period.
		Current employees are required to complete information security awareness training annually.	Inspected the information security awareness training completion form for a sample of current employees to determine that current employees were required to complete information security awareness training annually.	No exceptions noted.
		Management tracks and monitors compliance with information security and awareness training requirements.	Inspected the information security awareness training completion form for a sample of current employees to determine that management tracked and monitored compliance with information security and awareness training requirements.	No exceptions noted.
		Prior to hire, personnel are required to acknowledge the employee handbook.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that prior to 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 and code of conduct when changes are made.	Inquired of the Senior Security Engineer regarding the employee handbook acknowledgement to determine that personnel were required to acknowledge the employee handbook and code of conduct when changes were made.	No exceptions noted.
			Inspected the employee handbook to determine that personnel were required to acknowledge the employee handbook and code of conduct when changes were made.	No exceptions noted.
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct when changes were made.	Testing of the control activity disclosed that there were no changes made to the employee handbook that required employee acknowledgement during the review period.
		Executive management meets at least annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the kickoff meeting slide deck 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.

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**
		Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inquired of the Senior Security Engineer regarding how employees and third parties report unethical behavior to determine that employees, third parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
			Inspected the entity's SharePoint and support site to determine that employees, third parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		Changes to job roles and responsibilities are communicated to personnel through the entity's SharePoint site.	Inspected the SharePoint site to determine that changes to job roles and responsibilities were communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place and made available to personnel through the entity's SharePoint site.	Inspected the incident response policies and procedures and the entity's SharePoint site to determine that documented escalation procedures for reporting system failures, incidents, concerns, and other complaints were in place and made available to personnel through the entity's SharePoint site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's SharePoint site.	Inspected the entity's SharePoint site to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's SharePoint site.	No exceptions noted.
		The entity's third-party agreements delineate the boundaries of the system and describes relevant system components.	Inspected the third-party agreement for a sample of third parties to determine that the entity's third-party agreements delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		The entity's third-party agreements communicate the system commitments and requirements of third parties.	Inspected the third-party agreement for a sample of third parties to determine that the entity's third-party agreements communicated the system commitments and requirements of third parties.	No exceptions noted.
		The entity's third-party agreements outline and communicate the terms, conditions, and responsibilities of third parties.	Inspected the third-party agreement for a sample of third parties to determine that the entity's third-party agreements outlined and communicated the terms, conditions, and responsibilities of third parties.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the SaaS subscription agreement template to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	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 executed agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
		The entity's contractor agreements outline and communicate the terms, conditions, and responsibilities of external users.	Inspected the contractor agreement template to determine that the entity's contractor agreements outlined and communicated the terms, conditions, and responsibilities of external users.	No exceptions noted.
		Changes to commitments, requirements and responsibilities are communicated to third parties, external users, and customers via website notices.	Inquired of the Senior Security Engineer regarding changes to commitments, requirements, and responsibilities to determine that changes to commitments, requirements and responsibilities were communicated to third parties, external users, and customers via website notices.	No exceptions noted.
			Inspected the release notes on the entity's website to determine that changes to commitments, requirements and responsibilities were communicated to third parties, external users, and customers via website notices.	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**
		Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place and shared with external parties.	Inspected the third-party agreement for a sample of third parties 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.
		Executive management meets at least annually with operational management to discuss the results of assessments performed by third parties.	Inspected the Cybersecurity Tabletop meeting slide deck, notes, and meeting invite to determine that executive management met at least annually with operational management to discuss the results of assessments performed by third parties.	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, the employee performance evaluation 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 SMART.	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the risk assessment 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 reviews policies, procedures, and other control documents for alignment to the entity's objectives on an annual basis.	Inspected the revision history of the entity's policies and procedures to determine that executive management reviewed policies, procedures, and other control documents for alignment to the entity's objectives on an annual basis.	No exceptions noted.
		Executive management reviews and addresses control failures.	Inspected the Cybersecurity Tabletop meeting slide deck, notes, and meeting invite to determine that executive management reviewed and addressed control failures.	No exceptions noted.
			Inquired of the Senior Security Engineer regarding the internal controls failures to determine that executive management reviewed and addressed control failures.	No exceptions noted.
			Inspected the security governance policies and procedures to determine that executive management reviewed and addressed control failures.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of internal control failures to determine that executive management reviewed and addressed control failures.	Testing of the control activity disclosed that no control failures were identified during the review period.

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 controls effectiveness, including the acceptable level of control operation and failure.	Inspected the key performance indicators for operational 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.
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the security governance policies and procedures to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.
		The entity has defined the desired level of performance and operation in order to achieve the established entity objectives.	Inspected the key performance indicators for operational and internal controls effectiveness to determine that the entity had defined the desired level of performance and operation in order to achieve the established entity 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**
		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 key performance indicators for business and employee performance 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.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the FY24 kickoff meeting slide deck 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 FY24 kickoff meeting slide deck to determine that entity strategies, objectives and budgets were assessed on an annual basis.	No exceptions noted.
		The entity's internal controls framework is based on a recognized framework.	Inspected the internal controls matrix to determine that the entity's internal controls framework was based on a recognized framework.	No exceptions noted.
		The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures.	Inquired of the Senior Security Engineer regarding the internal controls environment to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures.	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 internal controls matrix and the security governance policies and procedures 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 FY24 kickoff meeting slide deck to determine that applicable law, regulation, standard and legislature requirements were identified and integrated into the entity's strategies and objectives.	No exceptions noted.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk assessment 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 policies and procedures to determine that management had defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A formal risk assessment is performed on 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.
		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 for each identified vulnerability	Inspected the risk assessment policies and procedures to determine that the entity's risk assessment process included: • Identifying the relevant information assets that were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks 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 were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks 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 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.
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk assessment policies and procedures to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
			Inspected the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment policies and procedures to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			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 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.
			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.
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the risk assessment policies and procedures to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of 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 the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	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 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 risk assessment inclusive of fraud risk to determine that on an annual basis, management identified and assessed the types of fraud that could impact their business and operations.	No exceptions noted.

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

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

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**
		Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment 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 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.
		Changes in vendor and third-party relationships are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment policies and procedures to determine that changes in vendor and third-party relationships 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 in vendor and third-party relationships 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 settings, the change detection and monitoring software configurations, the IDPS configurations, and the firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.	Inspected the revision history of the entity's 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 compliance and operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the internal controls matrix to determine that on an annual basis, management reviewed the controls implemented within the environment for compliance and operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.
		Logical access reviews are performed on at least an annual basis.	Inquired of the Senior Security Engineer regarding user access reviews to determine that logical access reviews were performed on at least an annual basis.	No exceptions noted.

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 access review for the in-scope systems to determine that logical access reviews were performed on at least an annual basis.	No exceptions noted.
		A data backup restoration test is performed on an annual basis.	Inquired of the Senior Security Engineer regarding restoration testing to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test results to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
		Internal and external vulnerability scans are performed at least annually, and remedial actions are taken where necessary.	Inquired of the Senior Security Engineer regarding internal and external vulnerability scans to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	No exceptions noted.
			Inspected the completed vulnerability scan results to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting documentation for a sample of vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	No exceptions noted.
		A third-party performs a penetration test at least annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test report to determine that a third-party performed a penetration test at least annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the completed evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation report and management's review 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.

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**
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	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.	Senior management assesses the results of the compliance, control and risk assessments performed on the environment.	Inspected the weekly security review meeting invite to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment.	No exceptions noted.
		Senior management is made aware of high-risk vulnerabilities, deviations and control failures/gaps identified as part of the compliance, control and risk assessments performed.	Inspected the weekly security review meeting invite to determine that senior management was made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	No exceptions noted.
		Vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment are communicated to those parties responsible for taking corrective actions.	Inspected the various assessments performed on the environment to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting documentation for a sample of vulnerabilities identified by the vulnerability scans to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inquired of the Senior Security Engineer regarding the deviations identified to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the vulnerability management policies and procedures to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools, and applications for compliance to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	Testing of the control activity disclosed that there were no deviations identified from the tool used to monitor key systems, tools, and applications for compliance during the review period.
			Inquired of the Senior Security Engineer regarding the control gaps to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the vulnerability management policies to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of control failures/gaps identified from the internal audit/compliance assessment to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	Testing of the control activity disclosed that there were no control gaps/failures identified from the internal audit/compliance assessment during the review period.
		Vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment are documented, investigated, and addressed.	Inspected the various assessments performed on the environment to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were documented, investigated, and addressed.	No exceptions noted.
			Inspected the supporting documentation for a sample of vulnerabilities identified by the vulnerability scans to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment 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**
			Inquired of the Senior Security Engineer regarding the deviations identified to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were documented, investigated, and addressed.	No exceptions noted.
			Inspected the vulnerability management policies and procedures to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were documented, investigated, and addressed.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools, and applications for compliance to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were documented, investigated, and addressed.	Testing of the control activity disclosed that there were no deviations identified from the tool used to monitor key systems, tools, and applications for compliance during the review period.

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**
			Inquired of the Senior Security Engineer regarding the control gaps to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were documented, investigated, and addressed.	No exceptions noted.
			Inspected the vulnerability management policies to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were documented, investigated, and addressed.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of control failures/gaps identified from the internal audit/compliance assessment to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were documented, investigated, and addressed.	Testing of the control activity disclosed that there were no control gaps/failures identified from the internal audit/compliance assessment during the review period.

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**
		Vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment are addressed by those parties responsible for taking corrective actions.	Inspected the various assessments performed on the environment to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting documentation for a sample of vulnerabilities identified by the vulnerability scans to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inquired of the Senior Security Engineer regarding the deviations identified to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment 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 vulnerability management policies and procedures to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools, and applications for compliance to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	Testing of the control activity disclosed that there were no deviations identified from the tool used to monitor key systems, tools, and applications for compliance during the review period.
			Inquired of the Senior Security Engineer regarding the control gaps to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment 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 vulnerability management policies and procedures to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of control failures/gaps identified from the internal audit/compliance assessment to determine that vulnerabilities, deviations, and control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	Testing of the control activity disclosed that there were no control gaps/failures identified from the internal audit/compliance assessment during the review period.
		Management tracks whether vulnerabilities, deviations and control failures/gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the weekly security review meeting invite to determine that management tracked whether vulnerabilities, deviations and control failures/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.	As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations, and control gaps.	Inspected the completed risk assessment and the internal controls matrix to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations, and control gaps.	No exceptions noted.
		Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	Inspected the various assessments performed on the environment to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the supporting documentation for a sample of vulnerabilities identified by the vulnerability scans to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/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**
			Inquired of the Senior Security Engineer regarding the deviations identified to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the vulnerability management policies and procedures to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of deviations identified from the tool used to monitor key systems, tools, and applications for compliance to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	Testing of the control activity disclosed that there were no deviations identified from the tool used to monitor key systems, tools, and applications for compliance during the review period.

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**
			Inquired of the Senior Security Engineer regarding the control gaps to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the vulnerability management policies and procedures to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of control failures/gaps to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	Testing of the control activity disclosed that there were no control gaps/failures identified from the internal audit/compliance assessment during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the 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.
		Prior to the development and implementation of internal controls into the environment, management considers the complexity, nature, and scope of its operations.	Inquired of the Senior Security Engineer regarding the internal controls environment to determine that prior to the development and implementation of internal controls into the environment, management considered the complexity, nature, and scope of its operations.	No exceptions noted.
			Inspected the internal controls matrix to determine that prior to the development and implementation of internal controls into the environment, management considered the complexity, nature, and scope of its operations.	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 Cybersecurity Tabletop meeting slide deck, notes, and meeting invite to determine that prior to the development and implementation of internal controls into the environment, management considered the complexity, nature, and scope of its operations.	No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the internal controls matrix to determine that management had 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 internal controls matrix to determine that management had incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment 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.

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 completed risk assessment and the internal controls matrix 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.
			Inquired of the Senior Security Engineer regarding the control gaps 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 vulnerability 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 supporting incident ticket for a sample of control failures/gaps to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Testing of the control activity disclosed that there were no control gaps/failures identified from the internal audit/compliance assessment during the review period.

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**
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery policies and procedures, including revision history 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 plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		An analysis of incompatible operational duties is performed at least on an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inquired of the Senior Security Engineer regarding the analysis of incompatible operational duties to determine that an analysis of incompatible operational duties was performed at least on an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	No exceptions noted.
			Inspected the organizational chart and internal controls matrix to determine that an analysis of incompatible operational duties was performed at least on an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	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 quarterly board meeting invite and agenda to determine that an analysis of incompatible operational duties was performed at least on an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	Inspected the internal controls matrix to determine that management documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	No exceptions noted.
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the internal controls matrix to determine that management had documented the controls implemented around the entity's technology infrastructure.	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 internal controls matrix to determine that management had established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.
		As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the completed risk assessment to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management.	No exceptions noted.
		The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Authentication of access • Protecting the entity's assets from external threats	Inspected the 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 • Authentication of access • Protecting the entity's assets from external threats	No exceptions noted.
		Management has established controls around the acquisition, development, and maintenance of the entity's technology infrastructure.	Inspected the internal controls matrix to determine that management had established controls around the acquisition, development, and maintenance of the entity's technology infrastructure.	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**
CC5.3	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 personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.
		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 the internal controls matrix to determine that management had 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 internal controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Process owners and management operate the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and the internal controls matrix to determine that process owners and management operated the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	No exceptions noted.
		Process owners and management investigate and troubleshoot control failures.	Inspected the completed risk assessment and the internal controls matrix to determine that process owners and management investigated and troubleshot control failures.	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**
			Inquired of the Senior Security Engineer regarding the control gaps to determine that process owners and management investigated and troubleshot control failures.	No exceptions noted.
			Inspected the vulnerability management policies and procedures to determine that process owners and management investigated and troubleshot control failures.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of control failures/gaps to determine that process owners and management investigated and troubleshot control failures.	Testing of the control activity disclosed that there were no control gaps/failures identified from the internal audit/compliance assessment during the review period.
		Effectiveness of the internal controls implemented within the environment are evaluated at least annually.	Inspected the Cybersecurity Tabletop meeting slide deck, notes, and meeting invite to determine that effectiveness of the internal controls implemented within the environment were evaluated at least annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
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 configurations, authentication, access, and security monitoring.	Inspected the security governance policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	No exceptions noted.
		An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the inventory listing of system assets and components to determine that an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
	Internal Network - Active Directory			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Security Engineer regarding network access to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the network user listing and access roles 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 authorized personnel.	Inquired of the Senior Security Engineer regarding administrative access to the network to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the network administrator listing and access roles to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
		The network is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the network password configurations to determine that the network was configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.
		Network users are authenticated via individually assigned user accounts and passwords.	Inquired of the Senior Security Engineer regarding the authentication of a user to the network to determine that network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Observed the authentication of a user to the network to determine that network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the network user listing and password configurations to determine that network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout configurations to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Network audit logging configurations are in place that include user activity and system events.	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the network audit logs to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Production Network - Azure Active Directory			
		Production network user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Security Engineer regarding production network access to determine that production network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the production network user listing and access roles to determine that production network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Production network administrative access is restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding production administrative access to the production network to determine that production network administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production network administrator listing and access roles to determine that production network administrative access was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production network is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the production network password configurations to determine that production servers were configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.
		Production network users are authenticated via individually assigned user accounts and passwords.	Inquired of the Senior Security Engineer regarding the authentication of a user to the production network to determine that production network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Observed the authentication of a user to the production network to determine that production network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the production network user listing and password configurations to determine that production network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production network account lockout configurations to determine that production network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Production network audit logging configurations are in place that include user activity and system events.	Inspected the production network audit logging configurations and an example production network audit log extract to determine that production network audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Production network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production network audit logs to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production network audit log extract to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Production Servers - Azure			
		Production servers user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Security Engineer regarding production servers access to determine that production servers user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the production server user listing and access roles to determine that production servers user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Production servers administrative access is restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding the administrative access to the production servers to determine that production servers administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production server administrator listing and access roles to determine that production servers administrative access was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production servers users are authenticated via individually assigned user accounts and passwords.	Inquired of the Senior Security Engineer regarding the authentication of a user to the production servers to determine that production servers users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Observed the authentication of a user to the production servers to determine that production servers users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the production server user listings and password configurations to determine that production servers users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Production servers account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production servers account lockout configurations to determine that production servers account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production servers audit logging configurations are in place that include user activity and system events.	Inspected the production server audit logging configurations and an example production server audit log extract to determine that production servers audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Production servers audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production servers audit logs to determine that production servers audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production server audit log extract to determine that production servers audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Database - Azure SQL Server			
		Production database user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Security Engineer regarding production database access to determine that production 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				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the production database user listing and access roles to determine that production database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Production database administrative access is restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding administrative access to the production database to determine that production database administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production database administrator listing and access roles to determine that production database administrative access was restricted to authorized personnel.	No exceptions noted.
		Production databases are configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the production database password configurations to determine that production databases were configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production databases users are authenticated via individually assigned user accounts and passwords.	Inquired of the Senior Security Engineer regarding the authentication of a user to the production databases to determine that production databases users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Observed the authentication of a user to the production database to determine that production databases users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the production database user listings and password configurations to determine that production databases users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Production databases account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production database account lockout configurations to determine that production databases account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production databases audit logging configurations are in place to log user activity and system events.	Inspected the production database audit logging configurations and an example production database audit log extract to determine that production databases audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Production databases audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production database audit logs to determine that the production databases audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production database audit log extract to determine that production databases audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Application(s) - Profisee			
		Production application user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Security Engineer regarding production application access to determine that production application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the production application user listing and access roles to determine that production application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Production application administrative access is restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding administrative access to the production application to determine that production application administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production application administrator listing and access roles to determine that production application administrative access was restricted to authorized personnel.	No exceptions noted.
		The production application is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the production application password configurations to determine that production application was configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production application users are authenticated via individually assigned user accounts and passwords.	Inquired of the Senior Security Engineer regarding the authentication of a user to the production application to determine that production application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Observed the authentication of a user to the production application to determine that production application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the production application user listing and password configurations to determine that production application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Production application account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production application account lockout configurations to determine that production application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production application audit logging configurations are in place to log user activity and system events.	Inspected the production application audit logging configurations and an example production application audit log extract to determine that production application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Production application audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production application audit logs to determine that production application audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production application audit log extract to determine that production application audit logs were maintained and available for review when needed.	No exceptions noted.
	Remote Access - Azure VPN Gateway			
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Senior Security Engineer regarding VPN access to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The ability to administer VPN access is restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding administrative access to the VPN to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
			Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
		VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system.	Inquired of the Senior Security Engineer regarding the authentication of a user to the VPN to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
			Observed the authentication of a user to the VPN to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding the entity's networks to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.
			Inspected the network diagram, the firewall rulesets, and the network security groups 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 IDPS.	Inspected the IDPS configurations, the firewall rule sets, and the network diagram to determine that data coming into the environment was secured and monitored through the use of firewalls and an IDPS.	No exceptions noted.
		A demilitarized zone (DMZ) is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ configurations to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.
		Server certificate-based authentication is used as part of the Secure Sockets Layer (SSL) / 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 SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Passwords and production data is stored in an encrypted format using software supporting the AES-256.	Inspected the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES-256.	No exceptions noted.
		Encryption keys are protected during generation, storage, use, and destruction.	Inquired of the Senior Security Engineer regarding the encryption keys to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
			Inspected the encryption cryptography policies and procedures to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
		Logical access reviews are performed on at least an annual basis.	Inquired of the Senior Security Engineer regarding user access reviews to determine that logical access reviews were performed on at least an annual basis.	No exceptions noted.
			Inspected the completed access review for the in-scope systems to determine that logical access reviews were performed on at least an annual basis.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Senior Security Engineer regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the hiring procedures, the in-scope 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 personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked from personnel as a component of the termination process.	Inquired of the Senior Security Engineer regarding the termination process to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
			Inspected the termination procedures, the in-scope user listings, and the user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 configurations, authentication, access, and security monitoring.	Inspected the security governance policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Senior Security Engineer regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, the in-scope 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 personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked from personnel as a component of the termination process.	Inquired of the Senior Security Engineer regarding the termination process to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the termination procedures, the in-scope user listings, and the user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews are performed on at least an annual basis.	Inquired of the Senior Security Engineer regarding user access reviews to determine that logical access reviews were performed on at least an annual basis.	No exceptions noted.
			Inspected the completed access review for the in-scope systems to determine that logical access reviews were performed on at least an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
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 configurations, authentication, access, and security monitoring.	Inspected the security governance policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Senior Security Engineer regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, the in-scope 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 personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked from personnel as a component of the termination process.	Inquired of the Senior Security Engineer regarding the termination process to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the termination procedures, the in-scope user listings, and the user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews are performed on at least an annual basis.	Inquired of the Senior Security Engineer regarding user access reviews to determine that logical access reviews were performed on at least an annual basis.	No exceptions noted.
			Inspected the completed access review for the in-scope systems to determine that logical access reviews were performed on at least an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
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 the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.	Inspected the data classification and secure disposal 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.
		A third-party purges data stored on cloud backups per a defined schedule.	Inspected the data disposal vendor's contract and completed attestation report to determine that third-party purged data stored on cloud backups per a defined schedule.	No exceptions noted.
		Data that is no longer required is disposed of and rendered unreadable to meet the entity's objectives.	Inspected the data classification and secure disposal policies and procedures to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the system log for an example request to dispose of data, purge a system, or physically destroy a system to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations and the firewall rulesets to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		VPN, SSL/TLS, and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that VPN, SSL/TLS, and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		VPN users are authenticated via multi-factor authentication prior to being granted remote access to the system.	Inquired of the Senior Security Engineer regarding the authentication of a user to the VPN to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
			Observed the authentication of a user to the VPN to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the VPN authentication configurations to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
		Server certificate-based authentication is used as part of the SSL/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 SSL/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 digital certificates 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.	Inquired of the Senior Security Engineer regarding VPN access to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the Senior Security Engineer the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access roles to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rule sets for a sample of production servers 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 firewall rule sets for a sample of production servers 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 IDPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDPS configurations to determine that an IDPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDPS is configured to notify personnel upon intrusion detection.	Inspected the IDPS notification configurations and an example alert notification to determine that the IDPS was configured to notify personnel upon intrusion detection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software configurations for a sample of workstations and servers to determine that antivirus software was installed on workstations and servers 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.	Inquired of the Senior Security Engineer regarding the antivirus updates to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
			Inspected the antivirus software configurations for a sample of laptops and servers 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 laptops and servers in real-time.	Inquired of the Senior Security Engineer regarding the antivirus scan schedule to determine that the antivirus software was configured to scan laptops and servers in real-time.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the antivirus software configurations for a sample of workstations and servers to determine that the antivirus software was configured to scan laptops and servers in real-time.	No exceptions noted.
		Data is stored in an encrypted format using software supporting the AES-256.	Inspected the encryption configurations for data at rest to determine that data was stored in an encrypted format using software supporting the AES-256.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the acceptable use policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media device configurations to determine that the use of removable media was prohibited by policy except when authorized by management.	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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
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 Senior Security Engineer regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access roles to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		Backup data is replicated offsite by a third-party vendor at least annually.	Inspected the contract with the offsite backup storage vendor to determine that backup media was replicated offsite by a third-party vendor at least annually.	No exceptions noted.
		System data is encrypted during the replication process between cloud environments.	Inspected the backup replication configurations and encryption configurations to determine that system data was encrypted during the replication process between cloud environments.	No exceptions noted.
		The ability to recall backed up data is restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding recalling backed up data to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of users with the ability to restore backups to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		VPN, SSL/TLS, and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that VPN, SSL/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 SSL/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 SSL/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.	Inquired of the Senior Security Engineer the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rule sets for a sample of production servers 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 firewall rule sets for a sample of production servers 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 and the firewall rulesets to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		An IDPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDPS configurations to determine that an IDPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The IDPS is configured to notify personnel upon intrusion detection.	Inspected the IDPS notification configurations and an example alert notification to determine that the IDPS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Data is stored in an encrypted format using software supporting the AES-256.	Inspected the encryption configurations for data at rest to determine that data was stored in an encrypted format using software supporting the AES-256.	No exceptions noted.
		Backup data is stored in an encrypted format.	Inspected the encryption configurations for backup data to determine that backup data was stored in an encrypted format.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the acceptable use policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media device configurations 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 an example mobile device to determine that mobile devices were protected through the use of secured, encrypted connections.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The ability to install applications and software on workstations is restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding the applications and software to determine that the ability to install applications and software on workstations was restricted to authorized personnel.	No exceptions noted.
			Inspected the denial notification to determine that a warning notification appeared when an employee attempted to download an application or software.	No exceptions noted.
		The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Senior Security Engineer regarding the change implementation process to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
			Inspected the listing of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
		Change detection and monitoring software is utilized to help detect unauthorized changes within the production environment.	Inspected the change detection and monitoring software configurations to determine that a change detection and monitoring software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The change detection and monitoring software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the change detection and monitoring software notification configurations and an example alert generated from the change detection and monitoring software to determine that the change detection and monitoring software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		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 and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software configurations for a sample of workstations and servers to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inquired of the Senior Security Engineer regarding the antivirus updates to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
			Inspected the antivirus software configurations for a sample of laptops and servers 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 laptops and servers in real-time.	Inquired of the Senior Security Engineer regarding the antivirus scan schedule to determine that the antivirus software was configured to scan laptops and servers in real-time.	No exceptions noted.
			Inspected the antivirus software configurations for a sample of workstations and servers to determine that the antivirus software was configured to scan laptops and servers in real-time.	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 security governance policies and procedures to determine that management had defined configuration standards in the information security policies and procedures.	No exceptions noted.
		Policies and procedures are in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the security governance policies and procedures to determine that policies and procedures were in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software settings, the change detection and monitoring software configurations, the IDPS configurations, and the firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and an example monitoring system alert, the change detection and monitoring software notification configurations and an example alert generated from the change detection and monitoring software, the IDPS notification configurations, and an example IDPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		An IDPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDPS configurations to determine that an IDPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDPS is configured to notify personnel upon intrusion detection.	Inspected the IDPS notification configurations and an example alert notification to determine that the IDPS was configured to notify personnel upon intrusion detection.	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**
		Change detection and monitoring software is utilized to help detect unauthorized changes within the production environment.	Inspected the change detection and monitoring software configurations to determine that a change detection and monitoring software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		The change detection and monitoring software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the change detection and monitoring software notification configurations and an example alert generated from the change detection and monitoring software to determine that the change detection and monitoring software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the acceptable use policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media device configurations to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rule sets for a sample of production servers 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 firewall rule sets for a sample of production servers 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.
		Internal and external vulnerability scans are performed at least annually, and remedial actions are taken where necessary.	Inquired of the Senior Security Engineer regarding internal and external vulnerability scans to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	No exceptions noted.
			Inspected the completed vulnerability scan results to determine that internal and external vulnerability scans were performed at least annually, 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**
			Inspected the supporting documentation for a sample of vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	No exceptions noted.
		A third-party performs a penetration test at least annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test report to determine that a third-party performed a penetration test at least annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
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 the detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security, incident management, and logging and monitoring policies and procedures to determine that policies and procedures were in place regarding the detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 settings, the FIM software configurations, the IDS/IPS configurations, and the firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and an example monitoring system alert, the change detection and monitoring software notification configurations and an example alert generated from the change detection and monitoring software, the IDPS notification configurations, and an example IDPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		An IDPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDPS 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 IDPS configurations to determine that an IDPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDPS is configured to notify personnel upon intrusion detection.	Inspected the IDPS notification configurations and an example alert notification to determine that the IDPS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Change detection and monitoring software is utilized to help detect unauthorized changes within the production environment.	Inspected the change detection and monitoring software configurations to determine that a change detection and monitoring software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		The change detection and monitoring software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the change detection and monitoring software notification configurations and an example alert generated from the change detection and monitoring software to determine that the change detection and monitoring software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rule sets for a sample of production servers 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 firewall rule sets for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software configurations for a sample of workstations and servers to determine that antivirus software was installed on workstations and servers 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.	Inquired of the Senior Security Engineer regarding the antivirus updates to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the antivirus software configurations for a sample of laptops and servers 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 laptops and servers in real-time.	Inquired of the Senior Security Engineer regarding the antivirus scan schedule to determine that the antivirus software was configured to scan laptops and servers in real-time.	No exceptions noted.
			Inspected the antivirus software configurations for a sample of workstations and servers to determine that the antivirus software was configured to scan laptops and servers in real-time.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the acceptable use policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
			Inspected the removable media device configurations to determine that the use of removable media was prohibited by policy except when authorized by management.	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**
	Internal Network - Active Directory			
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout configurations to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Network audit logging configurations are in place that include user activity and system events.	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the network audit logs to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained and available for review when 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**
	Production Network - Azure AD			
		Production network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production network account lockout configurations to determine that production network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Production network audit logging configurations are in place that include user activity and system events.	Inspected the production network audit logging configurations and an example production network audit log extract to determine that production network audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Production network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production network audit logs to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production network audit log extract to determine that production network audit logs were maintained and available for review when 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**
	Production Servers - Azure			
		Production servers account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production servers account lockout configurations to determine that production servers account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Production servers audit logging configurations are in place that include user activity and system events.	Inspected the production server audit logging configurations and an example production server audit log extract to determine that production servers audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Production servers audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production servers audit logs to determine that production servers audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production server audit log extract to determine that production servers audit logs were maintained and available for review when 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**
	Production Databases - Azure SQL Server			
		Production databases account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production database account lockout configurations to determine that production databases account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Production databases audit logging configurations are in place to log user activity and system events.	Inspected the production database audit logging configurations and an example production database audit log extract to determine that production databases audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Production databases audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production database audit logs to determine that the production databases audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production database audit log extract to determine that production databases audit logs were maintained and available for review when 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**
	Production Application - Profisee			
		Production application account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production application account lockout configurations to determine that production application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Production application audit logging configurations are in place to log user activity and system events.	Inspected the production application audit logging configurations and an example production application audit log extract to determine that production application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Production application audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production application audit logs to determine that production application audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production application audit log extract to determine that production application audit logs were maintained and available for review when needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response 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.
		The incident response and escalation procedures are reviewed 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 annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on severity.	Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on severity.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the supporting incident ticket for a sample of incidents to determine 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**
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the Senior Security Engineer regarding critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	Testing of the control activity disclosed that no critical security incidents were identified 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 resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inquired of the Senior Security Engineer regarding incidents that resulted in the unauthorized use of personal information to determine that incidents resulting in the unauthorized use or disclosure of personal information were communicated to the affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that incidents resulting in the unauthorized use or disclosure of personal information were communicated to the affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incidents that resulted in the unauthorized disclosure of personal information to determine that incidents resulting in the unauthorized use or disclosure of personal information were communicated to the affected users.	Testing of the control activity disclosed that no critical security incidents that resulted in the unauthorized disclosure of personal information were identified 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.	Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the incident response policies and procedures to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented incident response 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.	Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inquired of the Senior Security Engineer regarding the actions taken to address identified incidents 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.	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**
		Critical security incidents that result in a service/business operation disruption are communicated to those affected through creation of an incident ticket.	Inquired of the Senior Security Engineer regarding critical security incidents that resulted in service operation disruption to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through creation of an incident ticket.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through creation of an incident ticket.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incidents that resulted in a service/business operation disruption to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through creation of an incident ticket.	Testing of the control activity disclosed that no critical security incidents that resulted in a business/service operation disruption were identified during the review period.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine that resolution of 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**
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.	Inquired of the Senior Security Engineer regarding the actions taken to address identified incidents to determine that the remediation actions taken for security 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 the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the Senior Security Engineer regarding critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and 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 security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	Testing of the control activity disclosed that no critical security incidents were identified during the review period.
		The risks associated with identified vulnerabilities are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the supporting documentation for a sample of vulnerabilities identified by the vulnerability scans to determine that the risks associated with the identified vulnerability were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
			Inspected the completed risk assessment to determine that the risks associated with identified vulnerabilities were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.

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**
		Management reviews reports at least on at least an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the Cybersecurity Tabletop meeting slide deck, notes, and meeting invite to determine that management reviewed reports at least on at least an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	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.
			Inspected the change ticket for an example incident that required a permanent fix 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 security governance, incident, business continuity and disaster recovery, 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.	Inquired of the Senior Security Engineer regarding 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.
			Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	Testing of the control activity disclosed that the entity does not have a formal backup policies and procedures in place.
		A data backup restoration test is performed on an annual basis.	Inquired of the Senior Security Engineer regarding the restoration testing to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed backup restoration test results to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
		Management reviews reports at least on at least an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the Cybersecurity Tabletop meeting slide deck, notes, and meeting invite to determine that management reviewed reports at least on at least an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the Senior Security Engineer regarding critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and 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 security incident analysis for a sample of critical security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	Testing of the control activity disclosed that no critical security incidents were identified during the review period.
		A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the business continuity and disaster recovery policies and procedures to determine that a business continuity and disaster recovery plan were documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations.	No exceptions noted.
		The business continuity and disaster recovery plan are tested on an annual basis.	Inspected the completed business continuity and disaster recovery plan test results to determine that the business continuity and disaster recovery plan were tested on an annual basis.	No exceptions noted.
		The business continuity and disaster recovery plan are updated based on business continuity and disaster recovery plan test results.	Inspected the business continuity and disaster recovery policies and procedures, including revision history, and the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plan were updated based on business continuity and 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 - Quality Assurance 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 - Quality Assurance Department • Implementation - Software Change Management Group	No exceptions noted.
		System changes are communicated to both affected internal and external users.	Inspected the change e-mail and release note on the entity's website to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The ability to migrate/merge changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Senior Security Engineer regarding the change implementation process to determine that the ability to migrate/merge changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
			Inspected the listing of users with the ability to migrate/merge changes into the production environment to determine that the ability to migrate/merge changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the supporting change ticket for a sample of system, firewall, and application 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 code repository 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 logically separated from the production environment.	Inspected the separate development, test, and production environments to determine that development and test environments were logically separated from the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System change requests are documented and tracked in a ticketing system.	Inspected the supporting change ticket for a sample of system, firewall, and application changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
		A code/peer review is systematically required prior to deploying the PR into the production environment.	Inspected the supporting change ticket for a sample of system, firewall, and application changes to determine that a code/peer review was systematically required prior to deploying the PR into the production environment.	No exceptions noted.
		Change detection and monitoring software is utilized to help detect unauthorized changes within the production environment.	Inspected the change detection and monitoring software configurations to determine that a change detection and monitoring software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		The change detection and monitoring software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the change detection and monitoring software notification configurations and an example alert generated from the change detection and monitoring software to determine that the change detection and monitoring software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

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**
		Back out procedures are documented to allow for rollback of application changes when changes impair system operation.	Inspected the code repository rollback capabilities to determine that back out procedures were documented to allow for rollback of application changes when changes impaired system operation.	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 system, firewall, and application 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.
		System changes implemented for remediating incidents follow the standard change management process.	Inspected the change management policies and procedures to determine that system changes implemented for remediating incidents followed the standard change management process.	No exceptions noted.
			Inspected the supporting change ticket for a sample of incidents to determine that system changes implemented for remediating incidents followed the standard change management process.	No exceptions noted.
		System patches/security updates follow the standard change management process.	Inspected the patch management policies and procedures to determine that system patches/security updates follow the standard patch management process.	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**
		System patches/security updates are performed on a configured schedule.	Inspected the system patching configurations and an example patching job to determine that system patches/security updates were performed on a configured schedule.	No exceptions noted.
		Security governance policies and procedures document the baseline requirements for the configuration of IT systems and tools.	Inspected the security governance policies and procedures to determine that security governance policies and procedures documented the baseline requirements for the 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 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 policies and procedures to determine that management had defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	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 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.
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk assessment policies and procedures to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
			Inspected the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment policies and procedures to determine that management developed risk mitigation strategies to address risks identified during the 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**
			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 had 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 management 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.
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the vendor risk management policies and procedures to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.

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 risk assessment inclusive of vendor risks 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 management policies and procedures to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
			Inspected the risk assessment inclusive of vendor risks to determine that identified third-party 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**
		The entity's third-party agreements outline and communicate: • 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 third-party agreement for a sample of third parties to determine that the entity's third-party agreements 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.
		Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation report and management's review 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 vendor risk assessment is performed on at least an annual basis which includes reviewing the activities performed by third parties.	Inspected the vendor risk management policies and procedures to determine that a vendor risk assessment was performed on at least an annual basis which included reviewing the activities performed by third parties.	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 risk assessment inclusive of vendor risks to determine that a vendor risk assessment was performed on at least an annual basis which included reviewing the activities performed by third parties.	No exceptions noted.
		Management has assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.	Inspected the vendor risk management policies and procedures to determine that management had assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.	No exceptions noted.
		Management has established exception handling procedures for services provided by third parties.	Inspected the vendor risk management policies and procedures to determine that management had established exception handling procedures for services provided by third parties.	No exceptions noted.
		The entity has documented procedures for addressing issues identified with third parties.	Inspected the vendor risk management policies and procedures to determine that the entity had documented procedures for addressing issues identified with third parties.	No exceptions noted.
		The entity has documented procedures for terminating third-party relationships.	Inspected the vendor risk management policies and procedures to determine that the entity had documented procedures for terminating third-party relationships.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(1)(i)	**Security management process:** Implement policies and procedures to prevent, detect, contain, and correct security violations.	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 preventing, detecting, containing, and correcting security violations.	Inspected the security governance policies and procedures and the incident response policies and procedures to determine policies and procedures were in place regarding preventing, detecting, containing, and correcting security violations.	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 settings, the change detection and monitoring software configurations, the IDPS configurations, and the firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and an example monitoring system alert, the change detection and monitoring software notification configurations and an example alert generated from the change detection and monitoring software, the IDPS notification configurations, and an example IDPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		An IDPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDPS configurations to determine that an IDPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDPS is configured to notify personnel upon intrusion detection.	Inspected the IDPS notification configurations and an example alert notification to determine that the IDPS was configured to notify personnel upon intrusion detection.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Change detection and monitoring software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the change detection and monitoring software configurations to determine that change detection and monitoring software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The change detection and monitoring software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the change detection and monitoring software notification configurations and an example alert generated from the change detection and monitoring software to determine that the change detection and monitoring software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
			Inspected the antivirus software configurations for a sample of workstations and servers to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Internal and external vulnerability scans are performed at least annually, and remedial actions are taken where necessary.	Inquired of the Senior Security Engineer regarding internal and external vulnerability scans to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	No exceptions noted.
			Inspected the completed vulnerability scan results to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	No exceptions noted.
			Inspected the supporting documentation for a sample of vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	No exceptions noted.
	Internal Network - Active Directory			
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout configurations to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network audit logging configurations are in place that include user activity and system events.	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the network audit logs to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Network - Azure AD			
		Production network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout configurations to determine that production network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production network audit logging configurations are in place that include user activity and system events.	Inspected the production network audit logging configurations and an example production network audit log extract to determine that production network audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Production network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production network audit logs to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production network audit log extract to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.
	Database - Azure SQL Server			
		Database configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production database account lockout configurations to determine that database account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database audit logging configurations are in place to log user activity and system events.	Inspected the production database audit logging configurations and an example production database audit log extract to determine that database audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Database audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production database audit logs to determine that the database audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production database audit log extract to determine that database audit logs were maintained and available for review when needed.	No exceptions noted.
	Application - Profisee			
		Application account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production application account lockout configurations to determine that application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application audit logging configurations are in place to log user activity and system events.	Inspected the production application audit logging configurations and an example production application audit log extract to determine that application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Application audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production application audit logs to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production application audit log extract to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(1)(ii)(A)	**Risk analysis:** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk assessment 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 policies and procedures to determine that management had defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating, and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	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.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**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 for each identified vulnerability	Inspected the risk assessment policies and procedures to determine that the entity's risk assessment process included: • Identifying the relevant information assets that were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks for each identified vulnerability	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**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 were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks for each identified vulnerability	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(1)(ii)(B)	**Risk management:** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). Factors identified in §164.306 include: • The size, complexity, capability of the covered entity • The covered entity's technical infrastructure • The costs of security measures • The probability and criticality of potential risks to ePHI	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 for each identified vulnerability	Inspected the risk assessment policies and procedures to determine that the entity's risk assessment process included: • Identifying the relevant information assets that were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks for each identified vulnerability	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**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 were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks for each identified vulnerability	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk assessment policies and procedures to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
			Inspected the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment 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.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		An IDPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDPS configurations to determine that an IDPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDPS is configured to notify personnel upon intrusion detection.	Inspected the IDPS notification configurations and an example alert notification to determine that the IDPS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Change detection and monitoring software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the change detection and monitoring software configurations to determine that change detection and monitoring software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The change detection and monitoring software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the change detection and monitoring software notification configurations and an example alert generated from the change detection and monitoring software to determine that the change detection and monitoring software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
			Inspected the antivirus software configurations for a sample of workstations and servers to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		Internal and external vulnerability scans are performed at least annually, and remedial actions are taken where necessary.	Inquired of the Senior Security Engineer regarding internal and external vulnerability scans to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	No exceptions noted.
			Inspected the completed vulnerability scan results to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting documentation for a sample of vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	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 rule sets for a sample of production servers 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 firewall rule sets for a sample of production servers 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.
164.308 (a)(1)(ii)(C)	**Sanction policy:** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the sanction policies within the employee handbook to determine that sanction policies, which included probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Internal Network - Active Directory			
164.308 (a)(1)(ii)(D)	**Information system activity review:** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Network audit logging configurations are in place that include user activity and system events.	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the network audit logs to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Network - Azure AD			
		Production network audit logging configurations are in place that include user activity and system events.	Inspected the production network audit logging configurations and an example production network audit log extract to determine that production network audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Production network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production network audit logs to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected an example production network audit log extract to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.
	Database - Azure SQL Server			
		Database audit logging configurations are in place to log user activity and system events.	Inspected the production database audit logging configurations and an example production database audit log extract to determine that database audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Database audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production database audit logs to determine that the database audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production database audit log extract to determine that database audit logs were maintained and available for review when needed.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Application - Profisee			
		Application audit logging configurations are in place to log user activity and system events.	Inspected the production application audit logging configurations and an example production application audit log extract to determine that application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Application audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production application audit logs to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production application audit log extract to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.
164.308 (a)(2)	**Assigned security responsibility:** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	Responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI is formally documented and assigned to a job role.	Inquired of the Senior Security Engineer regarding the responsibility for maintaining ePHI to determine that responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI was formally documented and assigned to a job role.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the Director of Technology job description and the organization chart to determine that responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI was formally documented and assigned to a job role.	No exceptions noted.
164.308 (a)(3)(i)	**Workforce security:** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under the Information Access Management standard and to prevent those who do not have appropriate access from obtaining access to ePHI. Policies and procedures should include Authorization and/or Supervision procedures, Workforce Clearance Procedure, and Termination Procedures.	Policies and procedures are formally defined and documented regarding accessing ePHI.	Inspected the security governance and data classification policies and procedures to determine that policies and procedures were formally defined and documented regarding accessing ePHI.	No exceptions noted.
		Users accessing ePHI are authenticated via individually-assigned user accounts and passwords to only authorized personnel.	Inquired of the Senior Security Engineer regarding the users access to ePHI to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Observed a user login to a network that maintains ePHI to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Inspected the network user listing and password configurations to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Access to ePHI is restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding access to ePHI to determine that access to ePHI was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of users with access to ePHI to determine that access to ePHI was restricted to authorized personnel.	No exceptions noted.
		Users with access to ePHI are reviewed by management on at least an annual basis.	Inquired of the Senior Security Engineer regarding user access reviews to determine that users with access to ePHI were reviewed by management on at least an annual basis.	No exceptions noted.
			Inspected the completed access review to determine that users with access to ePHI were reviewed by management on at least an annual basis.	No exceptions noted.
164.308 (a)(3)(ii)(A)	**Authorization and/or supervision:** Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Policies and procedures are formally defined and documented regarding authorization of access to ePHI.	Inspected the data classification policies and procedures to determine that policies and procedures were formally defined and documented regarding authorization of access to ePHI.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Senior Security Engineer regarding the hiring process to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the hiring procedures, the in-scope 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.
164.308 (a)(3)(ii)(B)	**Workforce clearance procedure:** Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Policies and procedures are formally defined and documented regarding accessing ePHI.	Inspected the security governance and data classification policies and procedures to determine that policies and procedures were formally defined and documented regarding accessing ePHI.	No exceptions noted.
		Users accessing ePHI are authenticated via individually-assigned user accounts and passwords to only authorized personnel.	Inquired of the Senior Security Engineer regarding the users access to ePHI to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Observed a user login to a network that maintains ePHI to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Inspected the network user listing and password configurations to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Access to ePHI is restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding access to ePHI to determine that access to ePHI was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of users with access to ePHI to determine that access to ePHI was restricted to authorized personnel.	No exceptions noted.
		Users with access to ePHI are reviewed by management on at least an annual basis.	Inquired of the Senior Security Engineer regarding user access reviews to determine that users with access to ePHI were reviewed by management on at least an annual basis.	No exceptions noted.
			Inspected the completed access review to determine that users with access to ePHI were reviewed by management on at least an annual basis.	No exceptions noted.
164.308 (a)(3)(ii)(C)	**Termination procedures:** Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [the Workforce Clearance Procedure] of this section.	Policies and procedures are formally defined and documented regarding revoking access following termination.	Inspected the security governance policies and procedures to determine that policies and procedures were formally defined and documented regarding revoking access following termination.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Senior Security Engineer regarding the termination process to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the termination procedures, the in-scope 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.
164.308 (a)(4)(i)	**Information access management:** Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of the Privacy Rule. Policies and procedures should include: Isolating Health Care Clearinghouse Functions, Access Authorization and Access Establishment and Modification.	Management maintains policies and procedures that ensure the authorization of access to ePHI and are consistent with the applicable requirements of the Privacy Rule.	Inquired of the Senior Security Engineer regarding the access requirements of the Privacy Rule to determine that management maintained policies and procedures that ensured the authorization of access to ePHI and were consistent with the applicable requirements of the Privacy Rule.	No exceptions noted.
			Inspected the security governance and data classification policies and procedures to determine that management maintained policies and procedures that ensured the authorization of access to ePHI and were consistent with the applicable requirements of the Privacy Rule.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(4)(ii)(A)	**Isolating healthcare clearinghouse functions:** If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Not applicable. The entity is not a healthcare clearinghouse.	Not applicable.	Not applicable.
164.308 (a)(4)(ii)(B)	**Access authorization:** Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.	Policies and procedures are formally defined and documented regarding authorization of access to ePHI.	Inspected the data classification policies and procedures to determine that policies and procedures were formally defined and documented regarding authorization of access to ePHI.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Senior Security Engineer regarding the hiring process to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, the in-scope 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.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(4)(ii)(C)	**Access establishment and modification:** Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Policies and procedures are formally defined and documented regarding authorization of access to ePHI.	Inspected the data classification policies and procedures to determine that policies and procedures were formally defined and documented regarding authorization of access to ePHI.	No exceptions noted.
		Access rights are reviewed for employees that transfer job function or role.	Inquired of the Senior Security Engineer regarding the job transfer procedures to determine that access rights were reviewed for employees that transfer job function or role.	No exceptions noted.
			Inspected the job transfer procedures, user access listings and user access change meeting invite for a sample of employees that transferred function or role employees to determine that access rights were reviewed for employees that transfer job function or role.	No exceptions noted.
		Users with access to ePHI are reviewed by management on at least an annual basis.	Inquired of the Senior Security Engineer regarding the user access reviews to determine that users with access to ePHI were reviewed by management on at least an annual basis.	No exceptions noted.
			Inspected the completed access review to determine that users with access to ePHI were reviewed by management on at least an annual basis.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(5)(i)	**Security awareness and training:** Implement a security awareness and training program for all members of the workforce (including management).	Executive management uses an outside vendor to assist with its continued training of employees.	Inspected the third-party agreement to determine that executive management used an outside vendor to assist with its continued training of employees.	No exceptions noted.
	Component of the Security Awareness and Training program should include Security Reminders, Protection Malicious Software, Log-in Monitoring and Password Management.	Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the professional development training catalog to determine that employees were required to attend continued training annually that related to their job role and responsibilities.	No exceptions noted.
			Inspected the training completion dashboard 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.
		Upon hire, employees are required to read and acknowledge the employee handbook and complete information security and awareness training.	Inspected the signed employee handbook and information security and awareness training meeting invite for a sample of new hires to determine that upon hire, employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Current employees are required to read and acknowledge the employee handbook, which contain information security policies and procedures, when changes are made.	Inquired of the Senior Security Engineer regarding the employee handbook acknowledgement to determine that current employees were required to read and acknowledge the employee handbook, which contain information security policies and procedures, when changes are made.	No exceptions noted.
			Inspected the employee handbook to determine that current employees were required to read and acknowledge the employee handbook, which contain information security policies and procedures, when changes are made.	No exceptions noted.
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that current employees were required to read and acknowledge the employee handbook, which contain information security policies and procedures, when changes are made.	Testing of the control activity disclosed that there were no changes made to the employee handbook that required employee acknowledgement during the review period.
		Current employees are required to complete information security and awareness training on an annual basis.	Inspected the information security awareness training completion form for a sample of current employees to determine that current employees were required to complete information security and awareness training on an annual basis.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(5)(ii)(A)	**Security reminders:** Periodic security updates.	Users are made aware of security updates and updates to security policies.	Inquired of the Senior Security Engineer regarding periodic security reminders to determine that users were made aware of security updates and updates to security policies.	No exceptions noted.
			Inspected the e-mail notification and Teams message to determine that users were made aware of security updates and updates to security policies.	No exceptions noted.
164.308 (a)(5)(ii)(B)	**Protection from malicious software:** Procedures for guarding against, detecting, and reporting malicious software.	Policies and procedures are formally documented regarding preventing, detecting, and reporting the presence of malicious software.	Inspected the security governance policies and procedures to determine that policies and procedures were formally documented regarding preventing, detecting, and reporting the presence of malicious software.	No exceptions noted.
		Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
			Inspected the antivirus software configurations for a sample of workstations and servers to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Internal Network - Active Directory			
164.308 (a)(5)(ii)(C)	**Log-in monitoring:** Procedures for monitoring log-in attempts and reporting discrepancies.	Network audit logging configurations are in place that include user activity and system events.	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the network audit logs to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Network - Azure AD			
		Production network audit logging configurations are in place that include user activity and system events.	Inspected the production network audit logging configurations and an example production network audit log extract to determine that production network audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Production network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production network audit logs to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected an example production network audit log extract to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.
	Database - Azure SQL Server			
		Database audit logging configurations are in place to log user activity and system events.	Inspected the production database audit logging configurations and an example production database audit log extract to determine that database audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Database audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production database audit logs to determine that the database audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production database audit log extract to determine that database audit logs were maintained and available for review when needed.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Application - Profisee			
		Application audit logging configurations are in place to log user activity and system events.	Inspected the production application audit logging configurations and an example production application audit log extract to determine that application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Application audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production application audit logs to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production application audit log extract to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.
164.308 (a)(5)(ii)(D)	**Password management:** Procedures for creating, changing, and safeguarding passwords.	Policies are in place to guide personnel in creating, changing, and safeguarding passwords.	Inspected the access control policies and procedures to determine that policies were in place to guide personnel in creating, changing, and safeguarding passwords.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Internal Network - Active Directory			
		The network is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the network password configurations to determine that the network was configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.
	Production Network - Azure AD			
		Production network is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the production network password configurations to determine that production servers were configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.
	Database - Azure SQL Server			
		Databases are configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the production database password configurations to determine that databases were configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Application - Profisee			
		The application is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the production application password configurations to determine that the application was configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.
164.308 (a)(6)(i)	**Security incident procedures:** Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.	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.	Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(6)(ii)	**Response and reporting:** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	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.
		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.	Inspected the incident management 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.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(7)(i)	**Contingency plan:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency.	Inspected the business continuity and disaster recovery policies and procedures to determine that a documented disaster recovery plan was in place to guide personnel in the event of an emergency.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
164.308 (a)(7)(ii)(A)	**Data backup plan:** Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Data backup policies and procedures are formally documented.	Inquired of the Senior Security Engineer regarding the backup policies and procedures to determine that data backup policies and procedures were formally documented.	No exceptions noted.
			Inspected the backup policies and procedures to determine that data backup policies and procedures were formally documented.	Testing of the control activity disclosed that the entity does not have formally documented backup policies and procedures in place.
		Full backups of certain application and database components are performed on at least a monthly basis and incremental backups are performed on a daily basis.	Inquired of the Senior Security Engineer regarding the full and incremental backups to determine that full backups of certain application and database components were performed on at least a monthly basis and incremental backups were performed on a daily basis.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the backup history logs for a sample of months to determine that full backups of certain application and database components were performed on at least a monthly basis and incremental backups were performed on a daily basis.	No exceptions noted.
164.308 (a)(7)(ii)(B)	**Disaster recovery plan:** Establish (and implement as needed) procedures to restore any loss of data.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency.	Inspected the business continuity and disaster recovery policies and procedures to determine that a documented disaster recovery plan was in place to guide personnel in the event of an emergency.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		Data backup restoration tests are performed on an annual basis.	Inquired of the Senior Security Engineer regarding the completed backup restoration test results to determine that data backup restorations were performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test results to determine that data backup restorations were performed on an annual basis.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(7)(ii)(C)	**Emergency Mode Operation Plan:** Establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency.	Inspected the business continuity and disaster recovery policies and procedures to determine that a documented disaster recovery plan was in place to guide personnel in the event of an emergency.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery plan test results to determine that business continuity and disaster recovery plans were 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 policies and procedures and the completed business continuity and disaster recovery plan 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.
164.308 (a)(7)(ii)(D)	**Testing and revision procedures:** Implement procedures for periodic testing and revision of contingency plans.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency.	Inspected the business continuity and disaster recovery policies and procedures to determine that a documented disaster recovery plan was in place to guide personnel in the event of an emergency.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery plan test results to determine that business continuity and disaster recovery plans were 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 policies and procedures and the completed business continuity and disaster recovery plan 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.
		Data backup restoration tests are performed on an annual basis.	Inquired of the Senior Security Engineer regarding the completed backup restoration test results to determine that data backup restorations were performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test results to determine that data backup restorations were performed on an annual basis.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(7)(ii)(E)	**Applications and data criticality analysis:** Assess the relative criticality of specific applications and data in support of another contingency plan component.	The entity maintains a policy to assess the relative criticality of applications, systems and other assets maintaining ePHI, so that such data can be properly protected during emergencies and during normal business operations.	Inspected the asset management policies and procedures to determine that the entity maintained a policy to assess the relative criticality of applications, systems and other assets maintaining ePHI, so that such data can be properly protected during emergencies and during normal business operations.	No exceptions noted.
		The entity maintains an asset inventory that categorizes and prioritizes systems and other assets maintaining ePHI.	Inspected the inventory listing of system assets and components to determine that the entity maintained an asset inventory that categorized and prioritized systems and other assets maintaining ePHI.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**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 for each identified vulnerability	Inspected the risk assessment policies and procedures to determine that the entity's risk assessment process included: • Identifying the relevant information assets that were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks for each identified vulnerability	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**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 were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks for each identified vulnerability	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(8)	**Evaluation:** Perform a periodic technical and nontechnical evaluation based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures meet the requirement.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency.	Inspected the business continuity and disaster recovery policies and procedures to determine that a documented disaster recovery plan was in place to guide personnel in the event of an emergency.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery plan test results to determine that business continuity and disaster recovery plans were 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 policies and procedures and the completed business continuity and disaster recovery plan 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.
		Internal and external vulnerability scans are performed at least annually, and remedial actions are taken where necessary.	Inquired of the Senior Security Engineer regarding internal and external vulnerability scans to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed vulnerability scan results to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	No exceptions noted.
			Inspected the supporting documentation for a sample of vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed at least annually, and remedial actions were taken where necessary.	No exceptions noted.
164.308 (b)(1)	**Business associate contracts and other arrangements:** A covered entity, in accordance with 164.306 [The Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with 164.314 [the Organization Requirements] that the business associate will appropriately safeguard the information.	Not applicable. The entity is not a covered entity.	Not applicable.	Not applicable.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (b)(2)	A business associate may permit a business that is a subcontractor to create, receive, maintain, or transmit ePHI on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.	Not applicable. The entity does not use subcontractors. The organization would not share ePHI if it was in their possession.	Not applicable.	Not applicable.
164.308 (b)(3)	**Written contract or other arrangement:** Document the satisfactory assurances required by paragraph (b)(1) or (b2) above of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a) [the Organizational Requirements].	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The boundaries of the system • System commitments and requirements • Terms, conditions, and responsibilities between the involved parties	Inquired of the Senior Security Engineer regarding business associate agreements to determine that the entity maintained business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions, and responsibilities between the involved parties	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the business associates agreement for a sample of business associates to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions, and responsibilities between the involved parties	No exceptions noted.
164.308 (b)(4)	**Arrangement:** Document the satisfactory assurances required by paragraph (b)(1) [the Business Associates Contracts and Other Arrangements] of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a).	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The boundaries of the system • System commitments and requirements • Terms, conditions, and responsibilities between the involved parties	Inquired of the Senior Security Engineer regarding business associate agreements to determine that the entity maintained business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions, and responsibilities between the involved parties	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the business associates agreement for a sample of business associates to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions, and responsibilities between the involved parties	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.310 (a)(1)	**Facility access controls:** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	This safeguard is the responsibility of the subservice organization. Refer to the Subservice Organizations section below for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (a)(2)(i)	**Contingency operations:** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency.	Inspected the business continuity and disaster recovery policies and procedures to determine that a documented disaster recovery plan was in place to guide personnel in the event of an emergency.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		Data backup restoration tests are performed on an annual basis.	Inquired of the Senior Security Engineer regarding the completed backup restoration test results to determine that data backup restorations were performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test results to determine that data backup restorations were performed on an annual basis.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.310 (a)(2)(ii)	**Facility security plan:** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	This safeguard is the responsibility of the subservice organization. Refer to the Subservice Organizations section below for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (a)(2)(iii)	**Access control and validation procedures:** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	This safeguard is the responsibility of the subservice organization. Refer to the Subservice Organizations section below for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (a)(2)(iv)	**Maintenance records:** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	This safeguard is the responsibility of the subservice organization. Refer to the Subservice Organizations section below for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (b)	**Workstation use:** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.	Procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI are in place.	Inquired of the Senior Security Engineer regarding the workstation environment to determine that procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI were in place. Inspected the acceptable use policies and procedures to determine that procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI were in place.	No exceptions noted. No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.310 (c)	**Workstation security:** Covered entities should implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.	Not applicable. The entity is not a covered entity.	Not applicable.	Not applicable.
164.310 (d)(1)	**Device and media control:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	This safeguard is the responsibility of the subservice organization. Refer to the Subservice Organizations section below for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (d)(2)(i)	**Disposal:** Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.	Inspected the data classification and secure disposal 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.	Inspected the data classification and secure disposal policies and procedures to determine data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the system log for an example request to dispose of data, purge a system, or physically destroy a system to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.310 (d)(2)(ii)	**Media re-use:** Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.	The entity sanitizes media containing ePHI when the media is to be re-used.	Inspected the data classification policies and procedures to determine that the entity sanitized media containing ePHI when the media was to be re-used.	No exceptions noted.
	Ensure that ePHI previously stored on electronic media cannot be accessed and reused. Identify removable media and their use. Ensure that ePHI is removed from reusable media before they are used to record new information.	Data that is no longer required for business purposes is rendered unreadable.	Inspected the data classification and secure disposal policies and procedures to determine data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the system log for an example request to dispose of data, purge a system, or physically destroy a system to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
164.310 (d)(2)(iii)	**Accountability:** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	This safeguard is the responsibility of the subservice organization. Refer to the Subservice Organizations section below for controls managed by the subservice organization.	Not applicable.	Not applicable.
164.310 (d)(2)(iv)	**Data backup and storage:** Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	Data backup policies and procedures are formally documented.	Inquired of the Senior Security Engineer regarding the backup policies and procedures to determine that data backup policies and procedures were formally documented.	No exceptions noted.
			Inspected the backup policies and procedures to determine that data backup policies and procedures were formally documented.	Testing of the control activity disclosed that the entity does not have a formal backup policies and procedures in place.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Full backups of certain application and database components are performed on at least a monthly basis and incremental backups are performed on a daily basis.	Inquired of the Senior Security Engineer regarding the full and incremental backups to determine that full backups of certain application and database components were performed on at least a monthly basis and incremental backups were performed on a daily basis.	No exceptions noted.
			Inspected the backup history logs for a sample of months to determine that full backups of certain application and database components were performed on at least a monthly basis and incremental backups were performed on a daily basis.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.312 (a)(1)	**Access control:** Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4) [Information Access Management].	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring.	Inspected the security governance policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	No exceptions noted.
		Users accessing ePHI are authenticated via individually-assigned user accounts and passwords to only authorized personnel.	Inquired of the Senior Security Engineer regarding the users access to ePHI to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Observed a user login to a network that maintains ePHI to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Inspected the network user listing and password configurations to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Senior Security Engineer regarding the hiring process to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the hiring procedures, the in-scope 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.
		Access to ePHI is restricted to authorized personnel.	Inquired of the Senior Security Engineer regarding access to ePHI to determine that access to ePHI was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of users with access to ePHI to determine that access to ePHI was restricted to authorized personnel.	No exceptions noted.
		Users with access to ePHI are reviewed by management on at least an annual basis.	Inquired of the Senior Security Engineer regarding user access reviews to determine that users with access to ePHI were reviewed by management on at least an annual basis.	No exceptions noted.
			Inspected the completed access review to determine that users with access to ePHI were reviewed by management on at least an annual basis.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the Senior Security Engineer regarding the termination process to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the termination procedures, the in-scope 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.
	Internal Network - Active Directory			
		Networks are configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity	Inspected the network password configurations to determine that networks were configured to enforce password requirements that included: • Password history • Password age (minimum & maximum) • Password length • Complexity	No exceptions noted.
	Production Network - Azure AD			
		Production network is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the production network password configurations to determine that production servers were configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Database - Azure SQL Server			
		Databases are configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity	Inspected the database password configurations to determine that database were configured to enforce password requirements that included: • Password history • Password age (minimum & maximum) • Password length • Complexity	No exceptions noted.
	Application - Profisee			
		The application is configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity	Inspected the application password configurations to determine that application was configured to enforce password requirements that included: • Password history • Password age (minimum & maximum) • Password length • Complexity	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.312 (a)(2)(i)	**Unique user identification:** Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user. Ensure that the necessary data is available in the system logs to support audit and other related business functions.	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring.	Inspected the security governance policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	No exceptions noted.
		Users accessing ePHI are authenticated via individually-assigned user accounts and passwords to only authorized personnel.	Inquired of the Senior Security Engineer regarding the users access to ePHI to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Observed a user login to a network that maintains ePHI to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Inspected the network user listing and password configurations to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Internal Network - Active Directory			
		The network is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the network password configurations to determine that the network was configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout configurations to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Network audit logging configurations are in place that include user activity and system events.	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the network audit logs to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected an example network audit log extract to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Network - Azure AD			
		Production network is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the production network password configurations to determine that production servers were configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.
		Production network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production network account lockout configurations to determine that production network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Production network audit logging configurations are in place that include user activity and system events.	Inspected the production network audit logging configurations and an example production network audit log extract to determine that production network audit logging configurations were in place that included user activity and system events.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production network audit logs to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production network audit log extract to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.
	Database - Azure SQL Server			
		Databases are configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity	Inspected the database password configurations to determine that database were configured to enforce password requirements that included: • Password history • Password age (minimum & maximum) • Password length • Complexity	No exceptions noted.
		Database account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production database account lockout configurations to determine that database account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database audit logging configurations are in place to log user activity and system events.	Inspected the production database audit logging configurations and an example production database audit log extract to determine that database audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Database audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the database audit logs to determine that the database audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production database audit log extract to determine that database audit logs were maintained and available for review when needed.	No exceptions noted.
	Application - Profisee			
		The application is configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity	Inspected the application password configurations to determine that application was configured to enforce password requirements that included: • Password history • Password age (minimum & maximum) • Password length • Complexity	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production application account lockout configurations to determine that application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Application audit logging configurations are in place to log user activity and system events.	Inspected the production application audit logging configurations and an example production application audit log extract to determine that application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Application audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production application audit logs to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production application audit log extract to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.312 (a)(2)(ii)	**Emergency access procedure:** Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency.	Inspected the disaster recovery plan to determine that a documented disaster recovery plan was in place to guide personnel in the event of an emergency.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
164.312 (a)(2)(iii)	**Automatic logoff:** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Workstations are configured to terminate inactive sessions after five minutes of inactivity. Users are required to re-validate with a username and password to gain control of the workstation.	Inquired of the Senior Security Engineer regarding the automatic logoff to determine that workstations were configured to terminate inactive sessions after five minutes of inactivity. Users were required to re-validate with a username and password to gain control of the workstation.	No exceptions noted.
			Observed a user inactive on their workstation for five minutes to determine that workstations were configured to terminate inactive sessions after five minutes of inactivity. Users were required to re-validate with a username and password to gain control of the workstation.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the security governance policies and procedures to determine that workstations were configured to terminate inactive sessions after five minutes of inactivity. Users were required to re-validate with a username and password to gain control of the workstation.	No exceptions noted.
			Inspected the desktop settings on a workstation; inactivity configurations; user account timeout configurations to determine that workstations were configured to terminate inactive sessions after five minutes of inactivity. Users were required to re-validate with a username and password to gain control of the workstation.	No exceptions noted.
164.312 (a)(2)(iv)	**Encryption and decryption:** Implement a mechanism to encrypt and decrypt ePHI.	VPN, SSL/TLS, and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that VPN, SSL/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 SSL/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 SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the Senior Security Engineer regarding the VPN authentication settings to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed a user authenticate to the VPN access to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			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.
164.312 (b)	**Audit controls:** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring.	Inspected the security governance policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Change detection and monitoring software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the change detection and monitoring software configurations to determine that change detection and monitoring software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The change detection and monitoring software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the change detection and monitoring software notification configurations and an example alert generated from the change detection and monitoring software to determine that the change detection and monitoring software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
	Internal Network - Active Directory			
		Network audit logging configurations are in place that include user activity and system events.	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the network audit logs to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected an example network audit log extract to determine that network audit logs were maintained and available for review when needed.	No exceptions noted.
	Production Network - Azure AD			
		Production network audit logging configurations are in place that include user activity and system events.	Inspected the production network audit logging configurations and an example production network audit log extract to determine that production network audit logging configurations were in place that included user activity and system events.	No exceptions noted.
		Production network audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production network audit logs to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production network audit log extract to determine that production network audit logs were maintained and available for review when needed.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Database - Azure SQL Server			
		Database audit logging configurations are in place to log user activity and system events.	Inspected the production database audit logging configurations and an example production database audit log extract to determine that database audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Database audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production database audit logs to determine that the database audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production database audit log extract to determine that database audit logs were maintained and available for review when needed.	No exceptions noted.
	Application - Profisee			
		Application audit logging configurations are in place to log user activity and system events.	Inspected the production application audit logging configurations and an example production application audit log extract to determine that application audit logging configurations were in place to log user activity and system events.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application audit logs are maintained and available for review when needed.	Inquired of the Senior Security Engineer regarding the production application audit logs to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.
			Inspected an example production application audit log extract to determine that application audit logs were maintained and available for review when needed.	No exceptions noted.
164.312 (c)(1)	**Integrity:** Implement policies and procedures to protect ePHI from improper alteration or destruction.	Policies and procedures are formally documented regarding protecting ePHI from improper alteration or destruction.	Inspected the data classification policies and procedures to determine that policies and procedures were formally documented regarding protecting ePHI from improper alteration or destruction.	No exceptions noted.
		VPN, SSL/TLS, and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that VPN, SSL/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 SSL/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 SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the Senior Security Engineer regarding the VPN authentication settings to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed a user authenticate to the VPN access to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			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.
		Change detection and monitoring software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the change detection and monitoring software configurations to determine that change detection and monitoring software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The change detection and monitoring software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the change detection and monitoring software notification configurations and an example alert generated from the change detection and monitoring software to determine that the change detection and monitoring software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the AES-256.	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using software supporting the AES-256.	No exceptions noted.
164.312 (c)(2)	**Mechanisms to authenticate ePHI:** Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	Policies and procedures are formally documented regarding protecting ePHI from improper alteration or destruction.	Inspected the data classification policies and procedures to determine that policies and procedures were formally documented regarding protecting ePHI from improper alteration or destruction.	No exceptions noted.
		VPN, SSL/TLS, and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that VPN, SSL/TLS, and other encryption technologies were used for defined points of connectivity.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**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 SSL/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 SSL/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.	Inquired of the Senior Security Engineer regarding the VPN authentication settings to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed a user authenticate to the VPN access to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			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.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Change detection and monitoring software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the change detection and monitoring software configurations to determine that change detection and monitoring software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The change detection and monitoring software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the change detection and monitoring software notification configurations and an example alert generated from the change detection and monitoring software to determine that the change detection and monitoring software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the AES-256.	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using software supporting the AES-256.	No exceptions noted.
164.312 (d)	**Person or entity authentication:** Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring.	Inspected the security governance policies and procedures to determine that documented policies and procedures were in place regarding system configurations, authentication, access, and security monitoring.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Users accessing ePHI are authenticated via individually-assigned user accounts and passwords to only authorized personnel.	Inquired of the Senior Security Engineer regarding the users access to ePHI to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Observed a user login to a network that maintains ePHI to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Inspected the network user listing and password configurations to determine that users accessing ePHI were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
	Network - Azure AD			
		Networks are configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity	Inspected the network password configurations to determine that networks were configured to enforce password requirements that included: • Password history • Password age (minimum & maximum) • Password length • Complexity	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Database - Azure SQL Server			
		Databases are configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity	Inspected the database password configurations to determine that database were configured to enforce password requirements that included: • Password history • Password age (minimum & maximum) • Password length • Complexity	No exceptions noted.
	Application - Profisee			
		The application is configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity	Inspected the application password configurations to determine that application was configured to enforce password requirements that included: • Password history • Password age (minimum & maximum) • Password length • Complexity	No exceptions noted.
164.312 (e)(1)	**Transmission security:** Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	Policies and procedures are formally documented regarding protecting electronically transmitted ePHI from unauthorized access.	Inspected the data classification policies and procedures to determine that policies and procedures were formally documented regarding protecting electronically transmitted ePHI from unauthorized access.	No exceptions noted.
		VPN, SSL/TLS, and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that VPN, SSL/TLS, and other encryption technologies were used for defined points of connectivity.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**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 SSL/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 SSL/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.	Inquired of the Senior Security Engineer regarding the VPN authentication settings to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed a user authenticate to the VPN access to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			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.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.312 (e)(2)(i)	**Integrity controls:** Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	Policies and procedures are formally documented regarding protecting electronically transmitted ePHI from improper alteration or destruction.	Inspected the data classification policies and procedures to determine that policies and procedures were formally documented regarding protecting electronically transmitted ePHI from improper alteration or destruction.	No exceptions noted.
		VPN, SSL/TLS, and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that VPN, SSL/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 SSL/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 SSL/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.	Inquired of the Senior Security Engineer regarding 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.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Observed a user authenticate to the VPN access to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			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.
164.312 (e)(2)(ii)	**Encryption:** Implement a mechanism to encrypt ePHI whenever deemed appropriate.	Policies and procedures are formally documented regarding the mechanisms used to encrypt ePHI.	Inspected the data classification policies and procedures to determine that policies and procedures were formally documented regarding the mechanisms used to encrypt ePHI.	No exceptions noted.
		VPN, SSL/TLS, and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that VPN, SSL/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 SSL/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 SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the Senior Security Engineer regarding the VPN authentication settings to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed a user authenticate to the VPN access to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			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.
		Critical data is stored in encrypted format using software supporting the AES-256.	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using software supporting the AES-256.	No exceptions noted.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.314 (a)(1)	**Business associate contracts or other arrangements:** A covered entity is not in compliance with the standards in § 164.502(e) if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful - (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary."	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The boundaries of the system • System commitments and requirements • Terms, conditions, and responsibilities between the involved parties	Inquired of the Senior Security Engineer regarding business associate agreements to determine that the entity maintained business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions, and responsibilities between the involved parties Inspected the business associates agreement for a sample of business associates to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions, and responsibilities between the involved parties	No exceptions noted. No exceptions noted.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.314 (a)(2)(i)	**Business Associate Contracts:** A business associate contract must provide that the business associate will: "Implement safeguards that protect the confidentiality, integrity, and availability of the electronic protected health; Report to the covered entity any security incident of which it becomes aware; Authorize termination of the contract, if the covered entity determines that the business associate has violated a material term of the contract."	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The boundaries of the system • System commitments and requirements • Terms, conditions, and responsibilities between the involved parties	Inquired of the Senior Security Engineer regarding business associate agreements to determine that the entity maintained business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions, and responsibilities between the involved parties Inspected the business associates agreement for a sample of business associates to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions, and responsibilities between the involved parties	No exceptions noted. No exceptions noted.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.314 (a)(2)(ii)	**Other Arrangement:** The Other Arrangements implementation specifications provide that when a covered entity and its business associate are both government entities, the covered entity may comply with the standard in either of two alternative ways: (1) if it enters into a memorandum of understanding (MOU) with the business associate and the MOU contains terms which accomplish the objectives of the Business Associate Contracts section of the Security Rule; or (2) if other law (including regulations adopted by the covered entity or its business associate) contain requirements applicable to the business associate that accomplish the objectives of the business associate contract.	Not applicable. The entity is not a government entity.	Not applicable.	Not applicable.
164.314 (b)(1)	**Requirements for Group Health Plans:** Except when the only ePHI disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	Not applicable. The entity is not a plan sponsor.	Not applicable.	Not applicable.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.314 (b)(2)	**Implementation Specifications:** The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to - (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and (iv) Report to the group health plan any security incident of which it becomes aware.	Not applicable. The entity is not a group health plan.	Not applicable.	Not applicable.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.316 (a)	**Policies and Procedures:** Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in 164.306(b)(2)(i), (ii), (iii), and (iv) [the Security Standards: General Rules, Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	The entity creates and implements appropriate policies and procedures as required by applicable legislations, regulators, and customers.	Inspected the security governance and the data classification policies and procedures to determine that the entity created and implemented appropriate policies and procedures as required by applicable legislations, regulators, and customers.	No exceptions noted.
		Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	Inspected the revision history of the entity's policies and procedures and the entity's SharePoint site to determine that policies and procedures were reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	No exceptions noted.
164.316 (b)(1)	**Documentation:** Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Policies and procedures are appropriately retained for a minimum of six (6) years from the date it was created or when it was last in effect, whichever is later.	Inquired of the Senior Security Engineer to determine that policies and procedures were appropriately retained for a minimum of six (6) years from the date when it was last in effect.	No exceptions noted.
			Inspected the security governance and the data classification policies and procedures to determine that policies and procedures were appropriately retained for a minimum of six (6) years from the date when it was last in effect.	No exceptions noted.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	Inspected the revision history of the entity's policies and procedures and the entity's SharePoint site to determine that policies and procedures were reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	No exceptions noted.
		Policies and procedures are created and maintained in written and electronic form.	Inspected the entity's policies and procedures to determine that policies and procedures were created and maintained in written and electronic form.	No exceptions noted.
164.316 (b)(1)(ii)	**Documentation:** if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	HIPAA related incidents and events are documented in a ticketing system.	Inspected the incident response policies and procedures to determine that HIPAA related incidents and events were documented in a ticketing system.	No exceptions noted.
164.316 (b)(2)(i)	**Time Limit:** Retain the documentation required by paragraph (b) (1) of this section for 6 years for the date of its creation or the date when it last was in effect, whichever is later.	Policies and procedures are appropriately retained for a minimum of six (6) years from the date it was created or when it was last in effect, whichever is later.	Inquired of the Senior Security Engineer to determine that policies and procedures were appropriately retained for a minimum of six (6) years from the date when it was last in effect.	No exceptions noted.
			Inspected the security governance and the data classification policies and procedures to determine that policies and procedures were appropriately retained for a minimum of six (6) years from the date when it was last in effect.	No exceptions noted.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.316 (b)(2)(ii)	**Availability:** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	Inspected the revision history of the entity's policies and procedures and the entity's SharePoint site to determine that policies and procedures were reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	No exceptions noted.
164.316 (b)(2)(iii)	**Updates:** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	Inspected the revision history of the entity's policies and procedures and the entity's SharePoint site to determine that policies and procedures were reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.402	Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.	Breach notification letters or e-mails are developed and prepared to be used during a breach of ePHI. Notification procedures include: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to covered entities when breach is discovered • Notice to the secretary of Human Health Services (HHS) and prominent media outlets about breaches involving more than 500 individual subject's records • Notice to next of kin about breaches involving parties who are deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records	Inquired of the Senior Security Engineer regarding breach notifications to determine that breach notification letters or e-mails were developed and prepared to be used during a breach of ePHI. Notification procedures included: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to Covered Entities when breach was discovered • Notice to the secretary of HHS and prominent media outlets about breaches that involved more than 500 individual subject's records • Notice to next of kin about breaches that involved parties who were deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response *Continued on next page*	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			• Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches that involved fewer than 500 patient records Inspected the incident response policies and procedures to determine that procedures were in place to guide personnel in developing breach notification letters or e-mails to be used during a breach of ePHI. Notification procedures included: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to Covered Entities when breach was discovered *Continued on next page*	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			• Notice to the secretary of HHS and prominent media outlets about breaches that involved more than 500 individual subject's records • Notice to next of kin about breaches that involved parties who were deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches that involved fewer than 500 patient records	

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected a sample of breaches of ePHI to determine that breach notification letters or e-mails were developed and prepared to be used during a breach of ePHI. Notification procedures included: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to Covered Entities when breach was discovered • Notice to the secretary of HHS and prominent media outlets about breaches that involved more than 500 individual subject's records • Notice to next of kin about breaches that involved parties who were deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches that involved fewer than 500 patient records	Testing of the control activity disclosed that no breaches of ePHI had occurred during the review period.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.404 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.
164.404 (2)	For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.
164.404 (b)	Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 days after discovery of a breach.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.404 (c)(1)	Elements of the notification required by paragraph (a) of this section shall include to the extent possible: (A) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) a description of the types of unsecured protected health information that were involved in the breach (Such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (C) any steps the individual should take to protect themselves from potential harm resulting from the breach; (D) a brief description of what the covered entity is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches; and (E) contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an e-mail address, website, or postal address.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.
164.404 (c)(2)	The notification required by paragraph (a) of this section shall be written in plain language.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.404 (d)(1)(i)	The notification required by paragraph (a) shall be provided in the following form: Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as more information becomes available.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.
164.404 (d)(1)(ii)	The notification required by paragraph (a) shall be provided in the following form: If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.404 (d)(2)	**Substitute notice**. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a substitute form of notice reasonable calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.
164.404 (d)(2)(i)	In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.404 (d)(2)(ii)	In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of the web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.
164.404 (d)(3)	In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.406	§164.406(a) For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. (b) Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. (c) The content of the notification required by paragraph (a) shall meet the requirements of §164.404(c).	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.
164.408 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.
164.408 (b)	For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, expect as provided in §164.412, provide the notification required by paragraph (a) contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS web site.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.408 (c)	For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in a manner specified on the HHS web site.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not applicable.	Not applicable.
164.410 (a)(1)	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	Breach notification letters or e-mails are developed and prepared to be used during a breach of ePHI. Notification procedures include: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to covered entities when breach is discovered • Notice to the secretary of Human Health Services (HHS) and prominent media outlets about breaches involving more than 500 individual subject's records *Continued on next page*	Inquired of the Senior Security Engineer regarding breach notifications to determine that breach notification letters or e-mails were developed and prepared to be used during a breach of ePHI. Notification procedures included: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to Covered Entities when breach was discovered *Continued on next page*	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		• Notice to next of kin about breaches involving parties who are deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records	• Notice to the secretary of HHS and prominent media outlets about breaches that involved more than 500 individual subject's records • Notice to next of kin about breaches that involved parties who were deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches that involved fewer than 500 patient records	

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that procedures were in place to guide personnel in developing breach notification letters or e-mails to be used during a breach of ePHI. Notification procedures included: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to Covered Entities when breach was discovered • Notice to the secretary of HHS and prominent media outlets about breaches that involved more than 500 individual subject's records • Notice to next of kin about breaches that involved parties who were deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response *Continued on next page*	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			• Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches that involved fewer than 500 patient records	

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected a sample of breaches of ePHI to determine that breach notification letters or e-mails were developed and prepared to be used during a breach of ePHI. Notification procedures included: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to Covered Entities when breach was discovered • Notice to the secretary of HHS and prominent media outlets about breaches that involved more than 500 individual subject's records • Notice to next of kin about breaches that involved parties who were deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches that involved fewer than 500 patient records	Testing of the control activity disclosed that no breaches of ePHI had occurred during the review period.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.410 (a)(2)	(2) For the purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).	The entity acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.	Inquired of the Senior Security Engineer regarding breach notification procedures to determine that procedures were in place to outline the responsibility of the entity personnel for notifying affected parties in the event of a breach of unsecured protected health information.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that procedures were in place to outline the responsibility of the entity personnel for notifying affected parties in the event of a breach of unsecured protected health information.	No exceptions noted.
			Inspected a sample of breaches of ePHI to determine that the entity acknowledged responsibility for notifying affected parties in the event of a breach of unsecured protected health information.	Testing of the control activity disclosed that no breaches of ePHI had occurred during the review period.
164.410 (b)	Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.	The entity notifies affected parties of a breach of ePHI no later than sixty (60) calendar days after the discovery of the breach.	Inquired of the Senior Security Engineer regarding breach notification procedures to determine that the entity notified affected parties of a breach of ePHI no later than sixty (60) calendar days after the discovery of the breach.	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that the entity maintained procedures to guide personnel in notifying affected parties of a breach of ePHI no later than sixty (60) calendar days after the discovery of the breach.	No exceptions noted.
			Inspected a sample of breaches of ePHI to determine that the entity maintained procedures to guide personnel in notifying affected parties of a breach of ePHI no later than sixty (60) calendar days after the discovery of the breach.	Testing of the control activity disclosed that no breaches of ePHI had occurred during the review period.
164.410 (c)(1)	The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired, used or disclosure during the breach.	The identification of each individual whose unsecured ePHI has been accessed during the breach is disclosed during notification procedures.	Inquired of the Senior Security Engineer regarding known breaches of ePHI to determine that the identification of each individual whose unsecured ePHI has been accessed during the breach was disclosed during notification procedures.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that procedures were in place to guide personnel in disclosing the identification of each individual whose unsecured ePHI was accessed during the breach.	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected a sample of breaches of ePHI to determine that the identification of each individual whose unsecured ePHI has been accessed during the breach was disclosed during notification procedures.	Testing of the control activity disclosed that no breaches of ePHI had occurred during the review period.
164.410 (c)(2)	A business associate shall provide the covered entity with any other information that the covered entity is required to include in the notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	Management provides the covered entity with any information that the covered entity is required to include in the notification to the individual at the time of the breach and as soon as it is available.	Inquired of the Senior Security Engineer regarding breach notification procedures to determine that management provided the covered entity with any information that the covered entity was required to include in the notification to the individual at the time of the breach and as soon as it was available.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that procedures were in place to guide management in providing the covered entity with any information that the covered entity was required to include in the notification to the individual at the time of the breach and as soon as it was available.	No exceptions noted.
			Inspected a sample of breaches of ePHI to determine that management provided the covered entity with any information that the covered entity was required to include in the notification to the individual at the time of the breach and as soon as it was available.	Testing of the control activity disclosed that no breaches of ePHI had occurred during the review period.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.412	If a law enforcement official states to a covered entity or business associate that a notification, notice or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	The entity refrains from, or delays notifying HHS personnel, the covered entity, or other required persons following the discovery of a breach of unsecured protected health information when required by law.	Inspected the incident response policies and procedures to determine that the entity maintained procedures to guide personnel in refraining from, or delaying notification to the HHS personnel, the covered entity, or other required persons following the discovery of a breach of unsecured protected health information when required by law.	No exceptions noted.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.414	**Administrative requirements and burden of proof**: (a) covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart. (b) In the event of a use or disclosure in violation of subpart E, the covered entity or business associate; as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosures did not constitute a breach as defined at §164.402. See §164.530 for definition of breach.	The entity acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.	Inspected the incident response policies and procedures to determine that procedures were in place to outline the responsibility of the entity personnel for notifying affected parties in the event of a breach of unsecured protected health information.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
CC1.2	Executive management evaluates the skills and expertise of its members 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 annually.	Testing of the control activity disclosed that a performance evaluation for one executive management member sampled was not documented. Inquired with the Senior Security Engineer regarding the executive management performance evaluation and determined the executive management member had a daily meeting repurposed to conduct this activity.	Profisee is currently in progress of reevaluating our Executive review process as part of our new HR processes.
CC1.4	The entity evaluates the competencies and experience of third parties prior to working with them.	Inspected the third-party review meeting invite for a sample of third parties to determine that the entity evaluated the competencies and experience of third parties prior to working with them.	Testing of the control activity disclosed that the entity did not evaluate the competencies and experience for one of three third parties sampled.	Profisee acknowledges this finding and will use it to improve and formalize our 3rd party review process to better capture this activity.
CC7.5	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.	Testing of the control activity disclosed that the entity does not have a formal backup policies and procedures in place.	Profisee does not currently have written formal backup policies, however these activities are documented and enforced by Terraform Infrastructure as Code. Profisee will take this finding and remediate by formalizing our backup policies and procedures as a written document separate from our IaaC solution.
164.308 (a)(7)(ii)(A), 164.310 (d)(2)(iv)	Data backup policies and procedures are formally documented.	Inspected the backup policies and procedures to determine that data backup policies and procedures were formally documented.	Testing of the control activity disclosed that the entity does not have formally documented backup policies and procedures in place.	