A-LIGN

Profisee Group, Inc.

Type 2 SOC 2 with HIPAA/HITECH

2023

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

January 1, 2023 to March 31, 2023

Table of Contents

SECTION 1

ASSERTION OF PROFISEE GROUP, INC. MANAGEMENT

ASSERTION OF PROFISEE GROUP, INC. MANAGEMENT

April 6, 2023

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 January 1, 2023 to March 31, 2023" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the 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 January 1, 2023 to March 31, 2023, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2023 to March 31, 2023, 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 January 1, 2023 to March 31, 2023, 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.

Nicholas W. Powell

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 January 1, 2023 to March 31, 2023" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2023 to March 31, 2023, 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 January 1, 2023 to March 31, 2023, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period January 1, 2023 to March 31, 2023, 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 January 1, 2023 to March 31, 2023, 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.

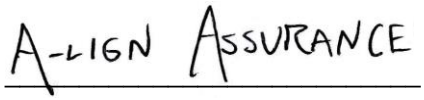
Restricted Use

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 January 1, 2023 to March 31, 2023, 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.



Tampa, Florida
April 6, 2023

SECTION 3

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

OVERVIEW OF OPERATIONS

Company Background

Microsoft developed and released Structured Query Language (SQL) Server Master Data Services (MDS) after acquiring Stratature in 2006. Principals at Stratature then created a new company - Profisee Group, Inc. (‘Profisee’) - to help more companies leverage enterprise master data management (MDM). As Microsoft developed its Azure ecosystem of cloud computer, storage, and analytics tools, it ceased development in MDS - and asked Profisee to embrace Azure and move off MDS as a code base in 2017. Profisee continues to elevate the MDM market with a commitment to being fast to deploy and easy to maintain allowing customers to solve their data problems quickly.

Profisee is a Microsoft Gold partner and is levered by firms in Financial Services, Telecommunications, Legal Services, Advertising, Manufacturing, Healthcare, Retail, Educational institutions.

Description of Services Provided

Profisee provides Database and File Management Software Services System 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 without 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 the new Software as a Service (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
Azure DevOps		Provides a central storage, assignment and tracking of development processes for the purpose of developing the Profisee Application

People

Profisee has approximately 120 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, Information Technology (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.
- **Research and Development** - Profisee*'s* Research and Development team is responsible for developing the Profisee Application, Testing of the applications and conducting activities for adding new features, integrations and support to the product.

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.

Profisee's headquarters location makes use of badge access and locks to prevent unapproved access to the location. Part of Profisee's limiting of risk to both Profisee and its customers is that Profisee does not store sensitive, internal or protected data at Profisee's Headquarters location.

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 the customer's own processes and able to be determined by the 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.

Profisee has also implemented Azure Privileged Identity Management to provide Just in Time Access style control over privileged roles within Azure. Activations are audited and reviewed regularly for justification, time the role was accessed and if the activation was part of an employee's duties.

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 failure over, and during annual testing has an average of 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 and Freshworks FreshService, 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, Premium Firewall, and Azure VPN. 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 and Horizon3 to provide a number of services, including Internal and External vulnerability scanning, Pentest/Red team engagements and 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.

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.

Access to Profisee's corporate network is controlled through Dell SonicWall and requires users to be in proper active directory groups and complete an MFA challenge prior to access being granted.

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 to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- 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 third-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 operates 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 Operating Officer (COO), Vice President of Information Services, Vice President of Operations, Vice President of Compliance, Vice President of Sales 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 Chief Technology Officer. 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 COO 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 on-going 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 in the Last 12 Months

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

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities since the organization 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.
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.
	CC6.4, 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 Categories

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

Control Activities Specified by the Service Organization

The applicable trust criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust criteria 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 that are not addressed by control activities at Profisee are described within Section 4 and within the Subservice Organization section above.

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, 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 restricting access, log visitors, and terminating 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 exists in order to protect 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; and
- 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, directives, guidelines, the code of conduct and the employee handbook.	Inspected the employee handbook and the entity's intranet to determine that core values were communicated from executive management to personnel through policies, directives, guidelines, 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.
		Upon hire, personnel are required to acknowledge the employee handbook.	Inspected the employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.
		Upon hire, personnel are required to sign a non-disclosure agreement.	Inspected the signed employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to sign a non-disclosure agreement.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to complete a background check.	Inspected background check policies and the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis.	No exceptions noted.
		Performance evaluations are performed for personnel on an annual basis.	Inquired of the Security Engineer regarding performance evaluation procedures to determine that performance evaluations were performed for personnel on an annual basis.	No exceptions noted.
			Inspected the performance evaluation form for a sample of current employees to determine that performance evaluations were performed for personnel on an annual basis.	Testing of the control activity disclosed that performance evaluation was not formally complete for seven of the twelve current employees sampled.
		Disciplinary policies, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the Employee handbook and the disciplinary policy and procedure to determine that sanction policies, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**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.	Inspected the entity e-mail address direction to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
			Inspected the harassment, reporting, anti-retaliation policies to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		The entity's third-party contract requires that third-parties have a code of conduct and employee handbook in place.	Inspected the third-party contract template to determine that the entity's third-party contract required that third-parties have a code of conduct and employee handbook in place.	No exceptions noted.
		Third-parties require their employees to complete a background check and acknowledge the employee handbook and code of conduct.	Inspected the third-party contract template to determine that third-parties required their employees to complete a background check and acknowledge the employee handbook and code of conduct.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities are documented and reviewed annually.	Inspected the executive management job descriptions including revision to determine that executive management roles and responsibilities were documented and reviewed 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**
		Executive management defines and documents the skills and expertise needed among its members.	Inspected the executive management job descriptions to determine that executive management defined and documented the skills and expertise needed among its members.	No exceptions noted.
		Executive management evaluates the skills and expertise of its members annually.	Inspected the performance evaluation schedule for an example of executive management members to determine that executive management evaluated the skills and expertise of its members annually.	No exceptions noted.
		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 operate the key controls within the environment.	No exceptions noted.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected meeting Modules to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management evaluates the skills and competencies of those that operate the internal controls within the environment annually.	Inquired of the Security Engineer regarding performance evaluation procedures to determine that executive management evaluated the skills and competencies of those that operate the internal controls within the environment annually.	No exceptions noted.
			Inspected the performance 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.	Testing of the control activity disclosed that performance evaluation was not formally complete for seven of the twelve current employees sampled.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the internal controls matrix to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.
			Inspected meeting Modules to determine that operational management assigned responsibility for and monitored 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**
		A third-party performs an independent assessment of the entity's controls environment annually to assess the effectiveness of internal controls within the environment.	Inspected the entity's completed attestation report to determine that a third-party performed an independent assessment of the entity's controls environment annually to assess the effectiveness of internal controls within the environment.	No exceptions noted.
		Outside executive council is brought in as needed to provide expertise and insight on the internal controls' environment.	Inspected a third-party contract to determine that outside executive council was brought in to provide expertise and insight on the internal controls environment.	No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary.	Inspected the revision history of the organizational chart to determine that executive management reviewed the organizational chart annually and made updates to the organizational structure and lines of reporting, if necessary.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management reviews job descriptions annually and makes updates, if necessary.	Inspected the revision history of the job description for a sample of job roles to determine that executive management reviewed job descriptions annually and made updates, if necessary.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct which requires adherence to the personnel's job role and responsibilities.	No exceptions noted.
		Executive management has established proper segregations of duties for key job functions and roles within the organization.	Inspected the organizational chart, internal controls matrix, and a sample of job descriptions to determine that executive management established proper segregations of duties for key job functions and roles within the organization.	No exceptions noted.
		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 management is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected vendor risk management policy to determine that a vendor risk assessment was required on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the risk assessment matrix to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.
		Executive management considers the roles and responsibilities performed by third-parties when documenting the organizational chart and defining job descriptions.	Inspected the organizational chart and the job description for a sample of job roles to determine that executive management considered the roles and responsibilities performed by third-parties when documenting the organizational chart and defining job descriptions.	No exceptions noted.
		Executive management considers interactions with, and the need to monitor the activities of third-parties when documenting the organizational chart and defining job descriptions.	Inspected the organizational chart, the job description for a sample of job roles, and the completed vendor risk assessment to determine that executive management considered interactions with, and the need to monitor the activities of third-parties when documenting the organizational chart and defining job descriptions.	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 are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee handbook to determine that policies were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance evaluations are performed for personnel on an annual basis.	Inquired of the Security Engineer regarding performance evaluation procedures to determine that performance evaluations were performed for personnel on an annual basis.	No exceptions noted.
			Inspected the performance evaluation form for a sample of current employees to determine that performance evaluations were performed for personnel on an annual basis.	Testing of the control activity disclosed that performance evaluation was not formally complete for seven of the twelve current employees sampled.
		The entity evaluates the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.	Inspected the interview questionnaire for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.	No exceptions noted.
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process.	Inspected the job description for a sample of job roles and resume for a sample of new hires to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process.	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's third-party contract requires that third-parties: • Consider the background, competencies and experience of its personnel • Provide regular training to its personnel as it relates to their job role and responsibilities	Inspected the customer agreement and third-party agreement templates to determine that the entity's third-party contract required that third-parties: • Consider the background, competencies and experience of its personnel • Provide regular training to its personnel as it relates to their job role and responsibilities	No exceptions noted.
			Inspected the third-party agreement for an example of third-parties and for a sample of customers to determine that it required the third-parties: • Consider the background, competencies and experience of its personnel • Provide regular training to its personnel as it relates to their job role and responsibilities	No exceptions noted.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the training completion certificates 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.

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 created a training program for its employees.	Inspected the information security and the training materials to determine that executive management created a training program for its employees.	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 relates to their job role and responsibilities.	No exceptions noted.
		The entity assesses training needs on an annual basis.	Inspected the training assessment to determine that the entity assessed the 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 training 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.
		Prior to employment, personnel are required to complete a background check.	Inspected background check policy and the completed background check for a sample of new hires to determine that prior to employment, personnel were required to complete a background check prior to employment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct which requires adherence to the personnel’s job role and responsibilities.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Policies are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee handbook to determine that policies were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		Executive management has established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities.	Inspected the employee 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 evaluations are performed for personnel on an annual basis.	Inquired of the Security Engineer regarding performance evaluation procedures to determine that performance evaluations were performed for personnel on an annual basis.	No exceptions noted.
			Inspected the performance evaluation form for a sample of current employees to determine that performance evaluations were performed for personnel on an annual basis.	Testing of the control activity disclosed that performance evaluation was not formally complete for seven of the twelve current employees 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**
		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 do not meet expectations as it relates to their job role and responsibilities.	No exceptions noted.
		Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary.	Inspected the revision history of the job description for a sample of job roles to determine that executive management reviewed the job requirements and responsibilities documented within job descriptions annually and made updates, if necessary.	No exceptions noted.
		Executive management reviews the responsibilities assigned to operational personnel annually and makes updates, if necessary.	Inspected meeting to determined that executive management reviewed the responsibilities assigned to operational personnel annually updates were made, as necessary.	No exceptions noted.
		Disciplinary policies, which include probation, suspension, and termination, are in place for employee misconduct.	Inspected the Employee handbook and the disciplinary policy and procedure to determine that sanction policies, which include probation, suspension, and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.	Inspected the information security policies and procedures, job description for a sample of job roles and the entity's intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inspected 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.
		Data flow diagrams, process flowcharts, narratives and procedures manuals are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected data flow diagrams, process flow charts, narratives and procedures manuals to determine that data flow diagrams, process flowcharts, narratives and procedures manuals 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 that entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inquired of the Security Engineer regarding FIM configurations, Intrusive Detective System (IDS) configurations, Intrusive Prevention System (IPS) configurations, encryption methods and 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.
			Inspected FIM configurations, IDS configurations, IPS configurations, encryption methods and configurations to determine that data entered into the system, processed by the system and output from the system was protected from unauthorized access.	No exceptions noted.
		Data and information critical to the system is assessed annually for relevance and use.	Inspected the data criticality assessment questionnaire to determine that data and information critical to the system was assessed annually for relevance and use.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's policies and procedures and employee handbook are made available to employees through the entity's intranet.	Inspected the entity's intranet to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to employees through the entity's intranet.	No exceptions noted.
		Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training.	Inspected the employee handbook, and information security and awareness training completion forms 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.
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.	Current employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis.	Inspected the employee handbook and information security and awareness training completion forms for a sample of current employees to determine that current employees were required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to acknowledge the employee handbook.	Inspected the employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.	Inspected the employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct which requires adherence to the personnel’s job role and responsibilities.	No exceptions noted.
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected meeting Modules 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.	Inspected the entity e-mail address direction to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
			Inspected the harassment, reporting, anti-retaliation policies 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 intranet.	Inspected the entity's intranet to determine that changes to job roles and responsibilities were communicated to personnel through the entity's intranet.	No exceptions noted.
		Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the entity's intranet.	Inspected incident response policy and the entity's intranet to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and made available to employees through the entity's intranet.	No exceptions noted.
		The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's intranet.	Inspected the entity's intranet to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's intranet.	No exceptions noted.

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 are required to attend security awareness training annually.	Inspected the employee handbook to determine that employees were required to attend security awareness training annually.	No exceptions noted.
			Inspected the training completion certificates for a sample of current employees to determine that employees were required to attend security awareness training annually.	No exceptions noted.
		Management tracks and monitors compliance with information security and awareness training requirements.	Inspected the security awareness training tracker for a sample of current employees to determine that management tracked and monitored compliance with information security and awareness training requirements.	No exceptions noted.
		The entity's third-party contract delineates the boundaries of the system and describes relevant system components.	Inspected the customer agreement and third-party contract templates to determine that the entity's third-party contract templates delineated the boundaries of the system and described relevant system components.	No exceptions noted.
			Inspected the third-party for an example of third-parties and for a sample of customers that the entity's third-party contract delineated the boundaries of the system and described relevant system components.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's third-party contract communicates the system commitments and requirements of third-parties.	Inspected the customer agreement and third-party contract templates to determine that the entity's third-party contract communicated the system commitments and requirements of third-parties.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users prior to allowing them access to the system.	Inspected the third-party contract for an example of third-parties and for a sample of customers to determine that the entity's third-party contract communicated the system commitments and requirements of third-parties.	No exceptions noted.
		The entity's third-party contract outlines and communicates the terms, conditions, and responsibilities of third-parties.	Inspected the entity's intranet to determine that the information security policies and procedures that communicate the system commitments and requirements of external users were provided to external users prior to allowing them access to the system.	No exceptions noted.
			Inspected the customer agreement and third-party contract templates to determine that the entity's third-party contract outlined and communicated the terms, conditions, and responsibilities of third-parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's contractor contract outlines and communicates the terms, conditions, and responsibilities of external users.	Inspected the third-party contract f for an example of third-parties and for a sample of customers to determine that the entity's third-party agreement 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 contractor contract template to determine that the entity's contractor contract outlined and communicated the terms, conditions, and responsibilities of external users.	No exceptions noted.
			Inspected the customer agreement template to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
		Changes to commitments, requirements and responsibilities are communicated to third-parties, external users, and customers via e-mails.	Inspected the third-party agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
		Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties.	Inspected the entity's e-mails, to determine that changes to commitments, requirements and responsibilities were communicated to third-parties, external users, and customers via e-mails.	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**
		Executive management meets annually with operational management to discuss the results of assessments performed by third-parties.	Inspected the incident response policy and the entity's intranet to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and shared with external parties.	No exceptions noted.
		Employees, third-parties and customers are directed on how to report unethical behavior in a confidential manner.	Inspected meeting Modules to determine that executive management met annually with operational management to discuss the results of assessments performed by third-parties.	No exceptions noted.
			Inspected the entity e-mail address direction to determine that an anonymous hotline was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
			Inspected the harassment, reporting, anti-retaliation policies 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				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.	Inspected the organizational chart, employee performance policies and procedures and the entity's documented objectives and strategies to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.
		Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART).	Inspected the entity's documented objectives and strategies to determine that executive management had documented objectives that were specific, measurable, attainable, relevant and time-bound (SMART).	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the risk management policy to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
			Inspected the risk assessment matrix 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 meeting Modules to determined 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 repeated control failures.	Inspected meeting Modules to determined that executive management reviewed and addressed repeated control failures.	No exceptions noted.
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.
		The entity has defined the desired level of performance and operation in order to achieve the established entity objectives.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that the entity defined the desired level of performance and operation in order to achieve the established entity objectives.	No exceptions noted.
		The operational reports reviewed by executive management define the acceptable level of operational performance and control failure.	Inspected operational reports to determine that the operational reports reviewed by executive management defined the acceptable level of operational performance and control failure.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the employee handbook and the meeting minutes 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.
			Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies.	No exceptions noted.
		Executive management reviews operational and resourcing reports to evaluate performance and resourcing at least annually.	Inspected the performance metrics to determine that executive management reviewed operational and resourcing reports to evaluate performance and resourcing at least annually.	No exceptions noted.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the entity's business plans, budget, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected meeting Modules to determine that entity strategies, objectives and budgets were assessed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management reviews key operational reports for precision and accuracy.	Inspected the performance metrics to determine that executive management reviewed key operational reports for precision and accuracy.	No exceptions noted.
		The entity's internal controls framework is based on a recognized (NIST 800-53; COBIT; ISO; COSO) framework.	Inspected compliance reports 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 Security Engineer regarding the internal controls matrix, policies and procedures related to the relevant statutory, regulatory, legislative and contractual requirements to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures.	No exceptions noted.
			Inspected the internal controls matrix, policies and procedures related to the relevant statutory, regulatory, legislative and contractual requirements to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures.	No exceptions noted.

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, policies and procedures related to the relevant statutory, regulatory, legislative and contractual requirements to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures.	Testing of the control activity disclosed no relevant statutory, regulatory, legislative and contractual requirements were in place during the review period.
		Applicable law, regulation, standard and legislature requirements are identified and integrated into the entity's strategies and objectives.	Inquired of the Security Engineer regarding policies and determined that no strategies, policies and procedures related to the relevant statutory, regulatory, legislative and contractual requirements, and the current registry of relevant regulatory, statutory, legislative and contractual requirements to determine that applicable law, regulation, standard and legislature requirements were identified and integrated into the entity's strategies and objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the entity's documented objectives and strategies, policies and procedures related to the relevant statutory, regulatory, legislative and contractual requirements, and the current registry of relevant regulatory, statutory, legislative and contractual requirements to determine that applicable law, regulation, standard and legislature requirements were identified and integrated into the entity's strategies and objectives.	No exceptions noted.
			Inspected the entity's documented objectives and strategies, policies and procedures related to the relevant statutory, regulatory, legislative and contractual requirements, and the current registry of relevant regulatory, statutory, legislative and contractual requirements to determine that applicable law, regulation, standard and legislature requirements were identified and integrated into the entity's strategies and objectives.	Testing of the control activity disclosed no relevant statutory, regulatory, legislative and contractual requirements were in place during the review period.
		The entity undergoes compliance audits at least annually to show compliance to relevant laws, regulations and standards.	Inspected the entity's completed attestation reports to determine that the entity underwent compliance audits at least annually to show compliance to relevant laws, regulations and standards.	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**
		Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected risk management policy to determine that documented policy was in place to guide personnel when performing a risk assessment.	No exceptions noted.
		Management has defined a formal risk management 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 management policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the risk assessment matrix to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that the entity's risk assessment process included: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks • Identified for each identified vulnerability	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk management policy 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**
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.	Risks identified as a part of the risk assessment process are addressed using the mitigation risk strategy.	Inspected the risk assessment matrix to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
			Inspected the risk management policy to determine that risks identified as a part of the risk assessment process were addressed using the mitigation risk strategy.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk management process.	Inspected the risk assessment matrix to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Mitigate the risk • Exclusion • Accept the risk	No exceptions noted.
			Inspected the risk management policy to determine that management developed risk mitigation strategies to address risks identified during the risk management 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 matrix 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 risk management policy 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 matrix 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 risk management policy 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 matrix 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 risk management policy 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.
		On an annual basis, management identifies and assesses the types of fraud (e.g., fraudulent reporting, loss of assets, unauthorized system access, overriding controls) that could impact their business and operations.	Inspected the risk assessment matrix 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.
		Identified fraud risks are reviewed and addressed using one of the following strategies: • Mitigate the risk • Exclusion • Accept the risk	Inspected the risk assessment matrix to determine that, on an annual basis, management identified and assessed the types of fraud (e.g., fraudulent reporting, loss of assets, unauthorized system access, overriding controls) that could impact their business and operations.	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 risk assessment matrix to determine that identified fraud risks were reviewed and addressed using one of the following strategies: • Mitigate the risk • Exclusion • Accept the risk	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities.	Inspected the risk assessment matrix 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 threats and vulnerabilities that arise from the use of Information Technology (IT) (e.g., unauthorized access, inadequate segregation of duties, default accounts, inadequate password management, unauthorized changes).	Inspected the risk assessment matrix 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.
		Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment matrix to determine that as part of management's assessment of fraud risks, management considered threats and vulnerabilities that arise from the use of IT (e.g., unauthorized access, inadequate segregation of duties, default accounts, inadequate password management, unauthorized changes).	No exceptions noted.
			Inspected the risk management policy 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**
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment matrix 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 risk management policy 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 matrix 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 risk management policy 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 completed risk assessment to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
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.		Inspected the risk management policy 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.
			Inspected the risk assessment matrix 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 dashboard console, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.	Inspected the entity policies to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
			Inspected meeting Modules to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
		On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses.	Inspected meeting Modules to determine that on an annual basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.

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**
		Key systems, tools, and applications are reviewed internally for compliance against documented policies and procedures by operational management annually or continuously using a compliance monitoring tool.	Inspected the internal control matrix to determine that key systems, tools and applications were reviewed internally for compliance against documented policies and procedures by operational management annually or continuously using a compliance monitoring tool.	No exceptions noted.
			Inspected the internal control matrix to determine that key systems, tools and applications were reviewed internally for compliance against documented policies and procedures by operational management annually or continuously using a compliance monitoring tool.	No exceptions noted.
		Control self-assessments that include, but are not limited to logical access reviews, and backup restoration tests are performed on annual basis.	Inspected the access control policy to determine that control self-assessments that included, but were not limited to logical access reviews, and backup restoration tests were performed on at least an annual basis.	No exceptions noted.
		Vulnerability scans are performed annually on the environment to identify control gaps and vulnerabilities.	Inspected the completed vulnerability scan to determine that vulnerability scans were performed quarterly on the environment to identify control gaps and vulnerabilities.	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**
		Evaluations of policies, controls, systems, tools, applications, and third-parties for effectiveness and compliance is required at least annually.	Inspected the revision history of entity policies to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required at least annually.	No exceptions noted.
			Inspected meeting Modules to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required at least annually.	No exceptions noted.
			Inspected the entity's completed attestation reports to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required at least annually.	No exceptions noted.
			Inspected the risk assessment matrix to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required at least annually.	No exceptions noted.
			Inspected the risk assessment matrix to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required at least annually.	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 internal control matrix to determine that evaluations of policies, controls, systems, tools, applications and third-parties for effectiveness and compliance were required at least annually.	No exceptions noted.
		Management reviews the frequency of compliance evaluations annually and adjusts it based on changes to the environment and operational performance.	Inspected meeting Modules to determine that management reviewed the frequency of compliance evaluations annually and adjusted it based on changes to the environment and operational performance.	No exceptions noted.
		A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		A third-party performs an independent assessment of the controls environment annually to assess the effectiveness of controls within the environment.	Inspected the entity's completed attestation reports to determine that a third-party performed an independent assessment of the controls environment annually to assess the effectiveness of controls within the environment.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inquired of the Security Engineer regarding performance evaluation procedures to determine that performance evaluations were performed for personnel on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the performance evaluation form for a sample of current employees to determine that performance evaluations were performed for personnel on an annual basis.	Testing of the control activity disclosed that performance evaluation was not formally complete for seven of the twelve current employees sampled.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the risk assessment matrix 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 meeting Modules 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 controls gaps identified as part of the compliance, control and risk assessments performed.	Inspected meeting Modules 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.

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 gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions.	Inquired of the Security Engineer regarding the completed risk and compliance assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the completed risk and compliance assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected a supporting incident ticket for a sample of vulnerabilities identified from a penetration test to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected a 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 gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
		Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are documented, investigated, and addressed.	Inquired of the Security Engineer regarding the completed risk and compliance assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.
			Inspected the completed risk and compliance assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected a supporting incident ticket for a sample of vulnerabilities identified from a penetration test to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.
			Inspected a 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 gaps identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.
			Inspected the associated incident ticket for an example internal control that has failed to determine that vulnerabilities, deviations, and control gaps identified from the risk and compliance assessments were documented, investigated, and addressed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are addressed by those parties responsible for taking corrective actions.	Inquired of the Security Engineer regarding the completed risk and compliance assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the completed risk and compliance assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the associated incident ticket for an example internal control that has failed to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
		Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected meeting Modules to determine that management tracked whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed were addressed in a timely manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	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 risk assessment 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 gaps identified as part of the various evaluations (e.g., risk assessments, vulnerability scans) performed.	Inspected the completed risk and compliance assessments to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the supporting incident ticket for an example internal control that had failed to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations (e.g., risk assessments, vulnerability scans) performed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected a supporting incident for a sample of vulnerabilities identified from a penetration test to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and 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.	Inspected the control matrix to determine that prior to the development and implementation of internal controls into the environment, management considers the complexity, nature and scope of its operations.	No exceptions noted.
			Inspected meeting Modules to determine that prior to the development and implementation of internal controls into the environment, management considers 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**
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the controls matrix to determine that management incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk management policy to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the risk assessment 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.
			Inspected the associated incident ticket for an example internal control that had failed to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.

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 policy and disaster recovery policy to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the organizational chart and internal controls matrix to determine that an analysis of incompatible operational duties was performed on at least 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 controls matrix to determine that management documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Organizational and information security policies and procedures are documented and made available to employees through the entity's intranet.	Inspected the information security policies and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's intranet.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the controls matrix to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.
		As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the risk assessment matrix to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats	Inspected the controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats	No exceptions noted.
		Management has established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	Inspected the controls matrix to determine that management established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Organizational and information security policies and procedures are documented and made available to employees through the entity's intranet.	Inspected the information security policy and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's intranet.	No exceptions noted.
		The incident response policy and information security policies and procedures detail the day-to-day activities to be performed by personnel.	Inspected the incident response policy and the information security policies to determine that the incident response policy and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	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 implemented controls that are built into the organizational and information security policies and procedures.	Inspected the incident response policy, information security policies and internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.
		Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for an example of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.
		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 controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 information security policies and 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 risk assessment matrix to determine that process owners and management investigated and troubleshot control failures.	No exceptions noted.
			Inspected the associated incident ticket for an example internal control that had failed to determine that process owners and management investigated and troubleshot control failures.	No exceptions noted.
		Effectiveness of the internal controls implemented within the environment are evaluated annually.	Inspected meeting Modules to determine that effectiveness of the internal controls implemented within the environment were evaluated 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.	An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the inventory listing of resources to determine an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Security Engineer to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies, the security governance policy, the access control policy and to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
	Network (Microsoft Azure)			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

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 administrative access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer regarding network administrators to determine that network administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
		Networks are configured to enforce password requirements that include: • Password history • Password age (minimum) • Password length	Inspected the network password settings to determine that networks were configured to enforce password requirements that included: • Password history • Password age (minimum) • Password length	No exceptions noted.
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the network account lockout settings to determine that network account lockout settings were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.

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 audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events	Inspected the network audit logging settings and example network audit log extracts to determine that network audit logging configurations were in place that included: • Account logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer, regarding network audit logs to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example network audit log extracts to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
	Operating System (Application, Web, and Database Servers)			
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

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**
		Operating system administrative access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer regarding administrative access to determine that operating system administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
			Inspected the operating system administrator listing to determine that operating system administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
		Operating systems are configured to enforce password requirements that include: • Password history • Password age (minimum) • Password length	Inspected the operating system password settings to determine that operating systems were configured to enforce password requirements that included: • Password history • Password age (minimum) • Password length	No exceptions noted.
		Operating system account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

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**
		Operating system audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events	Inspected the operating system audit logging settings and example operating system audit log extracts to determine that operating system audit logging configurations were in place that included: • Account logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted.
		Operating system audit logs are maintained and reviewed as needed.	Inquired of management to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example operating system audit log extracts to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
	Database (Azure Structured Query Language (SQL))			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Database administrative access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer regarding administrative access to determine that database administrative access was restricted to user accounts accessible by appropriate and 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 database administrator listing to determine that database administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
		Databases are configured to enforce password requirements that include: • Password history: 0 • Password age: 0 • Password length: 12 minimum • Multi-factor authentication (MFA)	Inspected the database password settings to determine that database were configured to enforce password requirements that included: • Password history: 0 • Password age: 0 • Password length: 12 minimum • MFA	No exceptions noted.
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the database account lockout settings to determine that database account lockout settings 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**
		Database audit logging settings are in place that include: • Account logon events • Logon events • Process tracking • System events	Inspected the database audit logging settings and example database audit log extracts to determine that database audit logging configurations were in place that included: • Account logon events • Logon events • Process tracking • System events	No exceptions noted.
		Database audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding audit logs to determine that the database audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example database audit log extracts to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.
	Application			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Application administrative access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer, Grant Elliot on February 22, 2023, regarding administrative access to determine that application administrative access was restricted to user accounts accessible by appropriate and 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 application administrator listing to determine that application administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
		The application is configured to enforce password requirements that include: • Password history • Password age (minimum) • Password length	Inspected the application password settings to determine that application was configured to enforce password requirements that included: • Password history • Password age (minimum) • Password length	No exceptions noted.
		Application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the application account lockout settings to determine that application account lockout settings were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Application audit policy settings are in place that include: • Account logon events • Logon events • Process tracking • System events	Inspected the application audit logging settings and example application audit log extracts to determine that application audit logging configurations were in place that included: • Account logon events • Logon events • Process tracking • System events	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**
		Application audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding audit logs to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example application audit log extracts to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
	Remote Access			
		Virtual Private Network (VPN) user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		The ability to administer VPN access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer regarding administrative access to determine that the ability to administer VPN access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
			Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to user accounts accessible by appropriate and 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 users are authenticated via multi-factor authentication (username, password, and PIN/OTP/Token) prior to being granted remote access to the system.	Inspected the Jumpbox authentication settings to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inspected the network diagram and the firewall settings to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.
		Access into the environment by outside entities requires a valid user ID and password and invalid login attempts are configured to be logged.	Inspected the Jumpbox authentication settings, VPN audit logging configurations and an example audit log extract for VPN access to determine that access into the environment by outside entities required a valid user ID and password and invalid login attempts were configured to be logged.	No exceptions noted.
		Data coming into the environment is secured and monitored through the use of firewalls and an IDS.	Inquired of the Security Engineer regarding IDS configuration to determine that data coming into the environment was secured and monitored through the use of firewalls and an IDS.	No exceptions noted.
			Inspected IDS configurations, firewall rule sets and the network diagram to determine that data coming into the environment was secured and monitored through the use of firewalls and an IDS.	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 demilitarized zone (DMZ) is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.
		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 encryption configurations to determine that server certificate-based authentication was used as part of the SSL encryption with a trusted certificate authority.	No exceptions noted.
		Stored passwords are encrypted.	Inspected encryption configurations for data at rest to determine that stored passwords were encrypted.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the transparent data encryption.	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using transparent data encryption.	No exceptions noted.
		Encryption keys are protected during generation, storage, use, and destruction.	Inspected the encryption cryptography policy to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	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 restricts access to its environment using the following mechanisms: • Classifying data • User identification	Inspected the data classification policy, listings of users with access to the network, operating system, database and application, firewall rule sets to determine that the entity restricted access to its environment using the following mechanisms: • Classifying data • User identification	No exceptions noted.
		Control self-assessments that include logical access reviews are performed on at least an annual basis.	Inspected the completed users access reviews to determine that control self-assessments that included logical access reviews were performed on at least an annual basis.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, network, operating system, database, application, and VPN user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee 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**
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, network, operating system, database, application, and VPN user listings, and user access revocation ticket for an example 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.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies, the security governance policy, the access control policy and to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	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**
CC6.2	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.	Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, network, operating system, database, application, and VPN user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, network, operating system, database, application, and VPN user listings, and user access revocation ticket for an example 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.
		Control self-assessments that include logical access reviews are performed on at least an annual basis.	Inspected the completed users access reviews to determine that control self-assessments that included logical access reviews were performed on at least an annual basis.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Security Engineer to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies, the security governance policy, the access control policy and to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
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.	Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, network, operating system, database, application, and VPN user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, network, operating system, database, application, and VPN user listings, and user access revocation ticket for an example 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.

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**
		Access rights are reviewed for employees that transfer job function or role.	Inquired of the Security Engineer regarding transferred employees to determine that access rights were reviewed for employees that transfer job function or role.	No exceptions noted.
			Inspected the access control policy to determine that access rights were reviewed for employees that transfer job function or role.	No exceptions noted.
			Inspected the list of transferred employees, and user access change ticket 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.	Testing of the control activity disclosed that no transfers occurred during the review period.
		An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected meeting Modules to determine that an analysis of incompatible operational duties was performed annually, and where incompatible responsibilities were identified, compensating controls were put into place.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Security Engineer to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the completed users access reviews to determine that control self-assessments that included logical access reviews were performed on at least an annual basis.	No exceptions noted.
		Control self-assessments that include physical and logical access reviews are performed on at least an annual basis.	Inspected the completed user access reviews to determine that control self-assessments that included logical access reviews were performed on at least an annual basis.	No exceptions noted.
	Network (Azure)			
		Network access reviews are completed by management annually.	Inspected the network access reviews to determine that network access reviews were completed by management annually.	No exceptions noted.
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

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**
	Operating System (Application, Web, and Database Servers)			
		Operating system access reviews are completed by management annually.	Inspected the operating system access reviews to determine that operating system access reviews were completed by management annually.	No exceptions noted.
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Database (Azure SQL)			
		Database access reviews are completed by management annually.	Inspected the database access reviews for an example to determine that database access reviews were completed by management annually.	No exceptions noted.
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Application			
		Application access reviews are completed by management annually.	Inspected the application access reviews to determine that application access reviews were completed by management 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**
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Policies and procedures are in place to guide personnel in physical security activities.	Inspected physical security policy to determine that policies and procedures were in place to guide personnel in physical security activities.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section below 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.	Data that is no longer required for business purposes is rendered unreadable.	Inspected the secure disposal policy to determine data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
		Policies and procedures are in place for removal of media storing critical data or software.	Inspected the acceptable use policy to determine policies and procedures were in place for removal of media storing critical data or software.	No exceptions noted.
		Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.

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**
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	VPN, SSL and other encryption technologies are used for defined points of connectivity.	Inspected encryption configurations and Jumpbox authentication configurations to determine VPN, SSL and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		VPN users are authenticated via multi-factor authentication (username, password, and PIN/OTP/Token) prior to being granted remote access to the system.	Inspected the Jumpbox authentication settings to determine that VPN users were authenticated via multi-factor authentication (username, password, and PIN/OTP/Token) prior to being granted remote access to the system.	No exceptions noted.
		Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority.	Inspected encryption configurations to determine that server certificate-based authentication was used as part of the SSL 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 to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inspected the Jumpbox 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.

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**
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Security Engineer regarding logical access to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		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 network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall 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.

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**
		An Intrusion Detection and Prevention System (IDS) is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected IDS log extract and alert notification to determine that the IDS is configured to notify personnel upon intrusion detection.	No exceptions noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
			Inspected the antivirus configurations for a sample of workstations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
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 is configured to scan workstations on a weekly basis.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the TDE.	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using TDE.	No exceptions noted.
		A DMZ is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
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 Security Engineer regarding logical access to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		Backup media is rotated off-site by a third-party vendor weekly.	Inspected the contract with the offsite backup storage vendor to determine that backup media was rotated off-site by a third-party vendor weekly.	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 offsite backup tape rotation logs for a sample of weeks to determine that backup media was rotated off-site by a third-party vendor weekly.	No exceptions noted.
		The ability to recall backed up data is restricted to authorized personnel.	Inquired of the Security Engineer to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
			Inspected the list of users with the ability to recall backup media to determine that the ability to recall backed up data was restricted to authorized personnel.	No exceptions noted.
		The entity secures its environment using a multi-layered defense approach that includes firewalls, antivirus software and a DMZ.	Inspected the network diagram, configurations, firewall rule sets, antivirus settings, IDS and DMZ settings to determine that the entity secured its environment using a multi-layered defense approach that included firewalls, antivirus software and a DMZ.	No exceptions noted.
		VPN, SSL and other encryption technologies are used for defined points of connectivity.	Inspected encryption configurations to determine that server certificate-based authentication was used as part of the SSL 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**
		Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority.	Inspected the encryption configurations to determine that server certificate-based authentication was used as part of the SSL encryption with a trusted certificate authority.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inspected the jumpbox authentication settings to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall 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 network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.

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 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 NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
			Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected IDS log extract and alert notification to determine that the IDS is 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**
		Critical data is stored in encrypted format using software supporting the TDE.	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using TDE.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected encryption configurations for an example backup media to determine that backup media was stored in an encrypted format.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		Mobile devices (e.g., laptops, smart phones) are protected through the use of secured, encrypted connections.	Inspected the mobile device policy to determine that mobile devices were protected through the use of secured, encrypted connections.	No exceptions noted.
		A warning notification appears when an employee attempts to download an application or software.	Inspected the warning notification received when an employee attempted to download an application or software to determine that a warning notification appeared when an employee attempted to download an application or software.	No exceptions noted.

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 migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Security Engineer regarding administrative access to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
			Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
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.	File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment.	Inquired of the Security Engineer regarding FIM configurations to determine FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
			Inspected FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inquired of the Security Engineer regarding the FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

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 FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policy to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
			Inspected the antivirus configurations for a sample of workstations 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.

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.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on a weekly basis.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		Information assets, software, hardware, tools, and applications introduced into the environment are scanned for vulnerabilities and malware prior to implementation into the environment.	Inspected the security scan to determine that information assets, software, hardware, tools, and applications introduced into the environment were scanned for vulnerabilities and malware prior to implementation into the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Management has defined configuration standards in the information security policies and procedures.	Inspected the information security policies to determine that management had defined configuration standards in the information security policies and procedures.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software, an example log extract from the IDS and an example IDS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		Key systems, tools, and applications are reviewed internally for compliance against documented policies and procedures by operational management annually or continuously using a compliance monitoring tool.	Inspected the internal control matrix to determine that key systems, tools and applications were reviewed internally for compliance against documented policies and procedures by operational management annually or continuously using a compliance monitoring tool**.**	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**
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected IDS log extract and alert notification to determine that the IDS is configured to notify personnel upon intrusion detection.	No exceptions noted.
		File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment.	Inspected FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
			Inspected FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

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 FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the acceptable use policy to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			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 network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the firewall 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.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected information security and incident response policy to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		Internal and external vulnerability scans and penetration tests are performed on quarterly basis and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results and the completed penetration test results to determine that internal and external vulnerability scans and penetration tests were performed on quarterly basis and remedial actions were taken where necessary.	No exceptions noted.
		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 policy to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident response policy to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software, an example log extract from the IDS and an example IDS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS 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 IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected IDS log extract and alert notification to determine that the IDS is configured to notify personnel upon intrusion detection.	No exceptions noted.
		File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment.	Inquired of the Security Engineer regarding FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
			Inspected FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

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 FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		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 network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the 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 configurations for a sample of workstations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on a weekly basis.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations on a weekly 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**
		The entity's third-party contract requires third-parties to implement detective controls and provide notice if the third-party's environment is compromised.	Inspected the customer agreement and the third-party contract templates to determine that the entity's third-party contract required third-parties to implement detective controls and provide notice if the third-party's environment was compromised.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media devices to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
	Network			
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the network account lockout settings to determine that network account lockout settings were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Network audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events	Inspected the network audit logging settings and example network audit log extracts to determine that network audit logging configurations were in place that included: • Account logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer, to determine that network audit logs were maintained and reviewed as needed. Inspected example network audit log extracts to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted. No exceptions noted.
	Operating System (Application, Web, and Database Servers)			
		Operating system account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Operating system audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset Inspected the operating system audit logging settings and example operating system audit log extracts to determine that operating system audit logging configurations were in place that included: • Account logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted. No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Operating system audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected example operating system audit log extracts to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
	Database			
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the database account lockout settings to determine that database account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Database audit logging settings are in place that include: • Account logon events • Logon events • Process tracking • System events	Inspected the database audit logging settings and example database audit log extracts to determine that database audit logging configurations were in place that included: • Account logon events • Logon events • Process tracking • System events	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding audit logs to determine that the database audit logs were maintained and reviewed as needed. Inspected example database audit log extracts to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted. No exceptions noted.
	Application			
		Application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the application account lockout settings to determine that application account lockout settings were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Application audit policy settings are in place that include: • Account logon events • Logon events • Process tracking • System events	Inspected the application audit logging settings and example application audit log extracts to determine that application audit logging configurations were in place that included: • Account logon events • Logon events • Process tracking • System events	No exceptions noted.
		Application audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding audit logs to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected example application audit log extracts to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
		Management reviews reports on 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 meeting Modules to determine that management reviewed reports on 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.
		Management monitors the effectiveness of detection tools and controls implemented within the environment.	Inspected meeting Modules to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment, including detection tools and controls.	No exceptions noted.
		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 policy to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected Incident response policy to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the Incident response policy to determine that the incident response policy defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of security incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the supporting incident ticket for a sample of security incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inspected the supporting incident ticket for an example critical security incident to determine that an impact analysis was performed 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**
		Identified incidents are reviewed, monitored and investigated by an incident response team.	Inspected the supporting incident ticket for a sample of security incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
		Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Inspected the Incident response policy to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of security incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the Incident response policy 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.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the Incident response policy to determine 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 security incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inspected the supporting incident ticket for a sample of security incidents to determine 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**
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected Incident response policy to determine that the documented incident response policy was in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.
		Critical security incidents that result in a service/business operation disruption are communicated to those affected through e-mails.	Inquired of the Security Engineer regarding audit logs to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through e-mails.	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 e-mails.	No exceptions noted.
			Inspected the supporting incident e-mails for an example critical security incident 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 e-mails.	Testing of this control activity disclosed that no critical security incident occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of security incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of security incidents to determine that the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	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 response policy to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of security incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inspected the supporting incident ticket for an example critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
		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 incident ticket for a sample of vulnerabilities identified from a penetration test 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	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 risk assessment matrix to determine that the risks associated with identified vulnerabilities were addressed using one of the following strategies: • Mitigate the risk • Exclusion • Accept the risk	No exceptions noted.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the Incident response policy to determine that the incident response and was reviewed at least annually for effectiveness.	No exceptions noted.
		Management reviews reports on an annual basis summarizing incident, 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 meeting Modules to determine that management reviewed reports on an annual basis summarizing incident, 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.
		Change management requests are opened for incidents that require permanent fixes.	Inspected the change management policy 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**
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	Inspected the information security, incident response, and business continuity policy to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the disaster recovery policy to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		Control self-assessments that include backup restoration tests are performed on at least an annual basis.	Inspected the completed backup restoration test to determine that control self-assessments that included backup restoration tests were performed on at least an annual basis.	No exceptions noted.
		Management reviews reports on an annual basis summarizing incident, 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 meeting Modules to determine that management reviewed reports on an annual basis summarizing incident, 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.

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 security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inspected the supporting incident ticket for an example critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
		On an annual basis, preventative and detective controls are evaluated and changed as necessary.	Inspected meeting Modules to determine that on an annual basis, preventative and detective controls were evaluated and changed as necessary.	No exceptions noted.
			Inspected the entity's completed attestation report to determine that on an annual basis, preventative and detective controls were evaluated and changed as necessary.	No exceptions noted.
		After critical incidents are investigated and addressed, lessons learned are documented and analyzed, and incident response plans and recovery procedures are updated based on the lessons learned.	Inspected the supporting incident ticket for an example critical security incident and incident response policy to determine that after critical incidents were investigated and addressed, lessons learned were documented and analyzed, and incident response plans and recovery procedures were updated based on the lessons learned.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the business continuity and disaster recovery policy to determine that a business continuity and disaster recovery plan was documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations.	No exceptions noted.
		The disaster recovery plan is tested on an annual basis.	Inspected the completed disaster recovery test results to determine that the disaster recovery plan was tested on an annual basis.	No exceptions noted.
		The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results.	Inspected the business continuity and disaster recovery policies and disaster recovery test results to determine that the business continuity and disaster recovery plan and procedures were updated based on disaster recovery plan test results.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policy 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 policy 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 supporting change ticket for a sample of infrastructure, operating system, database and application changes 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**
		Access to implement changes in the production environment is restricted to authorized IT personnel.	Inspected the list of users with access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the supporting change ticket for a sample of infrastructure, operating system, database 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 prior code repository revert to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed.	No exceptions noted.
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System change requests are documented and tracked in a ticketing system.	Inspected the supporting change ticket for a sample of infrastructure, operating system, database and application changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inquired of the Security Engineer regarding FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
			Inspected FIM configurations to determine that FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		Back out procedures are documented within each change implementation to allow for rollback of changes when changes impair system operation.	Inspected the supporting change ticket for a sample of infrastructure, operating system, database and application changes to determine that back out procedures were documented within each change implementation to allow for rollback of changes when changes impair system operation.	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 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 infrastructure, operating system, database and application changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change.	No exceptions noted.
		System changes implemented to the production environment are evaluated for impact to the entity's objectives.	Inspected the supporting change ticket for a sample of infrastructure, operating system, database and application changes to determine that system changes implemented to the production environment were evaluated for impact to the entity's objectives.	No exceptions noted.
		System changes implemented for remediating incidents follow the standard change management process.	Inspected the change management policy 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 infrastructure, operating system, database and application changes to determine that system changes implemented for remediating incidents followed the standard change 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**
		Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.	Inspected the information security policy to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management policy 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 policy are in place to guide personnel in performing risk mitigation activities.	Inspected the risk management policy to determine that documented policy were in place to guide personnel in performing risk mitigation activities.	No exceptions noted.
		Management has defined a formal risk management 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 management policy to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the risk assessment matrix 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 management policy to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
			Inspected the risk assessment matrix 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**
		Risks identified as a part of the risk assessment process are addressed using the mitigation risk strategy.	Inspected the risk management policy to determine that risks identified as a part of the risk assessment process were addressed using the mitigation risk strategy.	No exceptions noted.
			Inspected the risk assessment matrix to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Mitigate the risk • Exclusion • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk management process.	Inspected the risk management policy to determine that management developed risk mitigation strategies to address risks identified during the risk management process.	No exceptions noted.
			Inspected the risk assessment matrix to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.	Inspected the vendor risk management policy to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.	No exceptions noted.
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the vendor risk management policy to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.
			Inspected the risk assessment matrix 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 management policy to determine that identified third-party risks were rated using a risk evaluation process and ratings are approved by management.	No exceptions noted.
			Inspected the risk assessment matrix to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the third-party backup attestation report to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
		A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements.	Inspected the vendor risk management policy to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements.	No exceptions noted.
		Management has established exception handling procedures for services provided by third-parties.	Inspected the vendor risk management to determine that management established exception handling procedures for services provided by third-parties.	No exceptions noted.
		The entity has documented procedures for addressing issues identified with third-parties.	Inspected the vendor management policy to determine that the entity documented procedures for addressing issues identified with third-parties.	No exceptions noted.
		The entity has documented procedures for terminating third-party relationships.	Inspected the vendor management policy to determine that the entity 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 are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.
		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 management and escalation policies and procedures to determine documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident policies and procedures to determine policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software, an example log extract from the IDS and an example IDS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected IDS log extract and alert notification to determine that the IDS is configured to notify personnel upon intrusion detection.	No exceptions noted.
		File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the FIM configurations to determine FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		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 production server to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall rule sets for a sample production server to determine 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.

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 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 configurations for a sample of workstations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on a weekly basis.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		Internal and external vulnerability scans and penetration tests are performed on at least an annual basis and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results and the completed penetration test results to determine that internal and external vulnerability scans and penetration tests were performed on at least an annual basis and remedial actions were taken where necessary.	No exceptions noted.

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:** an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI).	A formal risk assessment is performed on an annual basis to identify threats that could impair systems security, confidentiality, integrity, and availability of ePHI.	Inspected the Risk management policy to determine that a formal risk assessment was performed on an annual basis to identify threats that could impair systems security, confidentiality, integrity, and availability of ePHI.	No exceptions noted.
			Inspected the risk assessment matrix to determine that a formal risk assessment was performed on an annual basis to identify threats that could impair systems security, confidentiality, integrity, and availability of ePHI.	No exceptions noted.
164.308 (a)(1)(ii)(B)	**Risk management:** Ensures the company implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306. 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	Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the Risk management policy to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the risk assessment matrix 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**
		Internal and external vulnerability scans and penetration tests are performed on at least an annual basis and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results and the completed penetration test results to determine that internal and external vulnerability scans and penetration tests were performed on at least an annual basis and remedial actions were taken where necessary.	No exceptions noted.
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.	The entity maintains policy and procedure documents that outline the process of sanctioning personnel who fail to comply with the security policies and procedures.	Inquired of the Inquired of the Security Engineer regarding the sanctioning of personnel who fail to comply with security requirements to determine that the entity-maintained policy and procedure documents that outline the process of sanctioning personnel who fail to comply with the security policies.	No exceptions noted.
			Inspected the Employee handbook and the disciplinary policy to determine that the entity-maintained policy and procedure documents that outline the process of sanctioning personnel who fail to comply with the security policies and procedures.	No exceptions noted.
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.	Regular monitoring and review of logins and log-in attempts to the system is in place. Discrepancies and potentially inappropriate or illegal activities are reported to senior management, legal counsel and/or human resources, as appropriate.	Inspected the Logging and Monitoring Policy to determine that regular monitoring and review of logins and log-in attempts to the system was in place. Discrepancies and potentially inappropriate or illegal activities were reported to senior management, legal counsel and/or human resources, as appropriate.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Network			
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging settings and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer, to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
	Operating System			
		Operating system audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events	Inspected the operating system audit logging settings and example operating system audit log extracts to determine that operating system audit logging configurations were in place that included: • Account logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Operating system audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example operating system audit log extract to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
	Database			
		Database audit logging settings are in place that include: • Account logon events • Logon events • Process tracking • System events	Inspected the database audit logging settings and an example database audit log extract to determine that database audit logging configurations were in place that included: • Account logon events • Logon events • Process tracking • System events	No exceptions noted.
		Database audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding audit logs to determine that the database audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example database audit log extract to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Application			
		Application audit policy settings are in place that include: • Account logon events • Logon events • Process tracking • System events	Inspected the application audit logging settings and an example application audit log extract to determine that application audit logging configurations were in place that included: • Account logon events • Logon events • Process tracking • System events	No exceptions noted.
		Application audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding audit logs to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example application audit log extract to determine that application audit logs were maintained and reviewed as needed.	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 security incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the supporting incident ticket for a sample of security incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 entity.	Responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI is assigned to the Security Engineer.	Inquired of the Security Engineer regarding assigned security responsibility to determine that responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI was assigned to the Security Engineer.	No exceptions noted.
			Inspected the assign security responsibility policy to determine that responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI was assigned to the Security Engineer.	No exceptions noted.
164.308 (a)(3)(i)	**Workforce security:** Policies and procedures are implemented to ensure that all members of the workforce have appropriate access to ePHI, 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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies, the security governance policy, the access control policy and to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Control self-assessments that include logical access reviews are performed on at least an annual basis.	Inspected the completed users access reviews to determine that control self-assessments that included logical access reviews were performed 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**
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, network, operating system, database, application, and VPN user listings, and user access request ticket for a sample of new hire to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, network, operating system, database, application, and VPN user listings, and user access revocation ticket for an example 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.
		Access rights are reviewed for employees that transfer job function or role.	Inquired of the Security Engineer regarding transferred employees to determine that access rights were reviewed for employees that transfer job function or role.	No exceptions noted.
			Inspected the access control policy to determine that access rights were reviewed for employees that transfer job function or role.	No exceptions noted.
			Inspected the list of transferred employees, and user access change ticket 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.	Testing of the control activity disclosed that no transfers occurred during the review period.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Network			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Network administrative access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer regarding network administrative access to determine that network administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
	Operating System (Application, Web, and Database Servers)			
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Operating system administrative access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer regarding administrative access to determine that operating system administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the operating system administrator listing to determine that operating system administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
	Database			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		Database administrative access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer regarding administrative access to determine that database administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
			Inspected the database administrator listing to determine that database administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
	Application			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application administrative access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer, Grant Elliot on February 22, 2023, regarding administrative access to determine that application administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
			Inspected the application administrator listing to determine that application administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
	Remote Access			
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		The ability to administer VPN access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer regarding administrative access to determine that the ability to administer VPN access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
			Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Physical Access (Carve Out - Microsoft Azure)			
		Part of 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.
164.308 (a)(3)(ii)(A)	**Authorization and/or supervision:** Ensures the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies, the security governance policy, the access control policy and to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Control self-assessments that include physical and logical access reviews are performed on at least an annual basis.	Inspected the completed user access reviews to determine that control self-assessments that included logical access reviews were performed on at least an annual basis.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, network, operating system, database, application, and VPN user listings, and user access request ticket for a sample of new hire 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**
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, network, operating system, database, application, and VPN user listings, and user access revocation ticket for an example 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.
		Access rights are reviewed for employees that transfer job function or role.	Inquired of the Security Engineer regarding transferred employees to determine that access rights were reviewed for employees that transfer job function or role.	No exceptions noted.
			Inspected the access control policy to determine that access rights were reviewed for employees that transfer job function or role.	No exceptions noted.
			Inspected the list of transferred employees, and user access change ticket 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.	Testing of the control activity disclosed that no transfers occurred during the review period.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(3)(ii)(B)	**Workforce clearance procedure:** Access of a workforce member (employee or computing device) to ePHI is appropriate.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel.	Inspected the access authorization policy, the access establishment and modification policy, the workforce clearance procedure, and the termination procedure to determine that access control and role-based build procedures were in place to restrict access to systems that maintain ePHI to only authorized personnel.	No exceptions noted.
		Control self-assessments that include physical and logical access reviews are performed on at least an annual basis.	Inspected the completed user access reviews to determine that control self-assessments that included logical access reviews were performed on at least an annual basis.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, network, operating system, database, application, and VPN user listings, and user access request ticket for a sample of new hire to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, network, operating system, database, application, and VPN user listings, and user access revocation ticket for an example 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.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(3)(ii)(C)	**Termination procedures:** Ensure that access to ePHI is terminated as soon as possible when a workforce member's employment ends.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies, the security governance policy, the access control policy and the hiring and termination policy to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, network, operating system, database, application, and VPN user listings, and user access revocation ticket for an example 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:** Policies and procedures are implemented that ensure authorizing access to ePHI and 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 Security Engineer regarding the access requirements of the Privacy Rule to determine that management-maintained policies and procedures that ensured authorizing access to ePHI and were consistent with the applicable requirements of the Privacy Rule.	No exceptions noted.
			Inspected the access control policy to determine that management-maintained policies and procedures that ensured authorizing 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 ePHI 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.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel.	Inspected the access authorization policy, the access establishment and modification policy, the workforce clearance procedure, and the termination procedure to determine that access control and role-based build procedures were in place to restrict access to systems that maintain ePHI to only authorized personnel.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, network, operating system, database, application, and VPN user listings, and user access request ticket for a sample of new hire 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.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel.	Inspected the access authorization policy, the access establishment and modification policy, the workforce clearance procedure, and the termination procedure to determine that access control and role-based build procedures were in place to restrict access to systems that maintain ePHI to only authorized personnel.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, network, operating system, database, application, and VPN user listings, and user access request ticket for a sample of new hire to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, network, operating system, database, application, and VPN user listings, and user access revocation ticket for an example 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.
		Access rights are reviewed for employees that transfer job function or role.	Inquired of the Security Engineer regarding transferred employees to determine that access rights were reviewed for employees that transfer job function or 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 access control policy to determine that access rights were reviewed for employees that transfer job function or role.	No exceptions noted.
			Inspected the list of transferred employees, and user access change ticket 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.	Testing of the control activity disclosed that no transfers occurred during the review period.
		Control self-assessments that include physical and logical access reviews are performed on at least an annual basis.	Inspected the completed user access reviews to determine that control self-assessments that included logical access reviews were performed on at least an annual basis.	No exceptions noted.
164.308 (a)(5)(i)	**Security awareness and training:** Implement a security awareness and training program for all members of the workforce (including management). Component of the Security Awareness and Training program should include Security Reminders, Protection Malicious Software, Log-in Monitoring and Password Management.	Management conducts periodic security awareness training to establish the organization's commitments and requirements for employees.	Inquired of the Security Engineer regarding security awareness and training activities to determine that management conducted periodic security awareness training to establish the organization's commitments and requirements for employees.	No exceptions noted.
			Inspected the periodic security awareness e-mails to determine that management conducted periodic security awareness training to establish the organization's commitments and requirements for employees.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Policies are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee handbook to determine that policies were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training.	Inspected the employee handbook, and information security and awareness training completion forms for a sample of new hire 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.
		Employees are required to attend security awareness training annually.	Inspected the employee handbook to determine that employees were required to attend security awareness training annually.	No exceptions noted.
			Inspected the training completion certificates for a sample of current employees to determine that employees were required to attend security awareness training annually.	No exceptions noted.
164.308 (a)(5)(ii)(A)	**Security reminders:** Periodic security updates.	Users are made aware of security updates and updates to security policies via e-mail notifications.	Inquired of the Security Engineer regarding periodic security reminders to determine that users were made aware of security updates and updates to security policies via e-mail notifications.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the periodic security e-mail submission to employees to determine that users were made aware of security updates and updates to security policies via e-mail notifications.	No exceptions noted.
164.308 (a)(5)(ii)(B)	**Protection from malicious software:** Procedures for guarding against, detecting, and reporting malicious software.	A program of techniques, technologies, and methods to guard against, detect, and report the presence of malicious software is in place.	Inspected the Profisee Acceptable Use Policy to determine that a program of techniques, technologies, and methods to guard against, detect, and report the presence of malicious software was in place.	No exceptions noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
			Inspected the antivirus configurations for a sample of workstations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The antivirus software is configured to scan workstations on a weekly basis.	Inspected the antivirus settings to determine that the antivirus software was configured to scan workstations on a weekly basis.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected IDS log extract and alert notification to determine that the IDS is 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**
164.308 (a)(5)(ii)(C)	**Log-in monitoring:** Procedures for monitoring log-in attempts and reporting discrepancies.	Regular monitoring and review of logins and log-in attempts to the system is in place. Discrepancies and potentially inappropriate or illegal activities are reported to senior management, legal counsel and/or human resources, as appropriate.	Inspected the Logging and Monitoring Policy to determine that regular monitoring and review of logins and log-in attempts to the system was in place. Discrepancies and potentially inappropriate or illegal activities were reported to senior management, legal counsel and/or human resources, as appropriate.	No exceptions noted.
	Network			
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging settings and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example operating system audit log extract to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Operating System			
		Operating system audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events	Inspected the operating system audit logging settings and example operating system audit log extracts to determine that operating system audit logging configurations were in place that included: • Account logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted.
		Operating system audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example operating system audit log extract to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
	Database			
		Database audit logging settings are in place that include: • Account logon events • Logon events • Process tracking • System events	Inspected the database audit logging settings and an example database audit log extract to determine that database audit logging configurations were in place that included: • Account logon events • Logon events • Process tracking • System events	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding audit logs to determine that the database audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example database audit log extract to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.
	Application			
		Application audit policy settings are in place that include: • Account logon events • Logon events • Process tracking • System events	Inspected the application audit logging settings and an example application audit log extract to determine that application audit logging configurations were in place that included: • Account logon events • Logon events • Process tracking • System events	No exceptions noted.
		Application audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding audit logs to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example application audit log extract to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**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 security incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the supporting incident ticket for a sample of security incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
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 for network devices and servers.	Inspected the password management policy, the access authorization policy and the access establishment and modification policy to determine that policies were in place to guide personnel in creating, changing, and safeguarding passwords for network devices and servers.	No exceptions noted.
	Network			
		Networks are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length	Inspected the network password settings to determine that networks were configured to enforce password requirements that included: • Password history • Password age (minimum and maximum) • Password length	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Operating System (Application, Web, and Database Servers)			
		Operating systems are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length	Inspected the operating system password settings to determine that operating systems were configured to enforce password requirements that included: • Password history • Password age (minimum and maximum) • Password length	No exceptions noted.
	Database			
		Databases are configured to enforce password requirements that include: • Password history: 0 • Password age: 0 • Password length: 12 minimum • MFA	Inspected the database password settings to determine that database were configured to enforce password requirements that included: • Password history: 0 • Password age: 0 • Password length: 12 minimum • MFA	No exceptions noted.
	Application			
		The application is configured to enforce password requirements that include: • Password history • Password age (minimum) • Password length	Inspected the application password settings to determine that application was configured to enforce password requirements that included: • Password history • Password age (minimum) • Password length	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Remote Access			
		VPN users are authenticated via multi-factor authentication (username, password, and PIN/OTP/Token) prior to being granted remote access to the system.	Inspected the Jumpbox authentication settings to determine that VPN users were authenticated via multi-factor authentication (username, password, and PIN/OTP/Token) prior to being granted remote access to the system.	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 policy 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 at least annually for effectiveness.	Inspected Incident response policy to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the Incident response policy to determine that the incident response policy defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of security 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**
		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 security incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inspected the supporting incident ticket for an example critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
		Identified incidents are reviewed, monitored and investigated by an incident response team.	Inspected the supporting incident ticket for a sample of security incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
		Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inquired of the Security Engineer regarding audit logs to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and 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 identified and communicated to the affected users.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected incident ticket for an example critical security incident that resulted in unauthorized disclosure of personal information to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and communicated to the affected users.	Testing of this control activity disclosed that no critical security incident occurred during the review period.
		Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Inspected the incident response policies and procedures to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of security incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.

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 management and escalation policies and procedures to determine 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 at least annually for effectiveness.	Inspected the revision history of the incident response policies and procedures to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of security incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the supporting incident ticket for a sample of security incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inspected the supporting incident ticket for an example critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
		Identified incidents are reviewed, monitored and investigated by an incident response team.	Inspected the supporting incident ticket for a sample of security incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
		Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inquired of the Security Engineer regarding audit logs to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and 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 identified and communicated to the affected users.	No exceptions noted.
			Inspected incident ticket for an example critical security incident that resulted in unauthorized disclosure of personal information to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and communicated to the affected users.	Testing of this control activity disclosed that no critical security incident occurred during the review period.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Inspected the incident response policies and procedures to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate 178 containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of security incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
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.	Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.	Inspected the business continuity and disaster recovery plans to determine that a business continuity plan was documented and in place that outlined the range of disaster scenarios and steps the business would take in a disaster to ensure the timely resumption of critical business operations.	No exceptions noted.
		The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity plan was tested on an annual basis and included: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	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.	Procedures are in place to provide for complete, accurate, and timely storage of data.	Inspected entity policies to determine that procedures were in place to provide for complete, accurate, and timely storage of data.	No exceptions noted.
		The ways in which critical data are backed up and stored are documented and reviewed annually.	Inspected entity policies to determine that the ways in which critical data were backed up and stored were documented and reviewed annually.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected entity policies to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		Full backups of certain application and database components are performed on a weekly.	Inspected the backup schedule and configurations for an example critical system to determine that full backups of certain application and database components were performed on a daily basis and incremental backups were performed on a weekly basis.	No exceptions noted.
			Inspected the backup history logs for a sample of weeks to determine that full backups of certain application and database components were performed on a monthly basis and incremental backups were performed on a monthly basis.	No exceptions noted.
		When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure.	Inspected backup configurations and an example backup alert to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure.	No exceptions noted.
		Backup media is rotated off-site by a third-party vendor on a weekly basis.	Inspected the contract in place with the offsite backup storage vendor to determine that backup media was rotated off-site by a third-party vendor on a weekly basis.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data backed up is replicated to an offsite facility in real-time.	Inspected backup replication configurations to determine that data backed up was replicated to an offsite facility in real-time.	No exceptions noted.
		Backups of critical data are maintained securely offsite by a third-party.	Inspected the contract with the offsite backup storage vendor to determine that backups of critical data were maintained offsite by a third-party.	No exceptions noted.
			Inspected the attestation report of the backup storage vendor to determine backups of critical data were maintained offsite by a third-party.	No exceptions noted.
		Control self-assessments that include Backup restoration tests are performed on at least an annual basis.	Inspected the completed backup restoration test to determine that control self-assessments that included Backup restoration tests were performed on at least an annual 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.	Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The disaster recovery plan includes moving the business operations and supporting systems to a warm site.	Inspected the business continuity and disaster recovery plans to determine that the disaster recovery plan included moving the business operations and supporting systems to a warm site.	No exceptions noted.
		A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.	Inspected the business continuity and disaster recovery plans to determine that a business continuity plan was documented and in place that outlined the range of disaster scenarios and steps the business would take in a disaster to ensure the timely resumption of critical business operations.	No exceptions noted.
		The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity plan was tested on an annual basis and included: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data Backup restoration tests are performed at least annual.	Inspected the completed backup restoration test results to determine that data backup restorations were performed on an annual basis.	No exceptions noted.
		Redundant architecture is in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	Inspected the business continuity and disaster recovery plans and network diagram to determine that redundant architecture was in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	No exceptions noted.
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.	Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		The disaster recovery plan includes moving the business operations and supporting systems to a hot site.	Inspected the business continuity and disaster recovery plans to determine that the disaster recovery plan included moving the business operations and supporting systems to a hot site.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.	Inspected the business continuity and disaster recovery plans to determine that a business continuity plan was documented and in place that outlined the range of disaster scenarios and steps the business would take in a disaster to ensure the timely resumption of critical business operations.	No exceptions noted.
		The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity plan was tested on an annual basis and included: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	No exceptions noted.
		Data Backup restoration tests are performed at least annual.	Inspected the completed backup restoration test results to determine that data backup restorations were performed on an annual.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Redundant architecture is in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	Inspected the business continuity and disaster recovery plans and network diagram to determine that redundant architecture was in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	No exceptions noted.
164.308 (a)(7)(ii)(D)	**Testing and revision procedures:** Implement procedures for periodic testing and revision of contingency plans.	Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity plan was tested on an annual basis and included: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	No exceptions noted.
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 has defined what critical data is processed and how it is processed.	Inspected the Data Classification to determine the entity defined what data was processed and how it was processed.	No exceptions noted.
		Data and information critical to the system is assessed annually for relevance and use.	Inspected the data criticality assessment questionnaire to determine that data and information critical to the system was assessed annually for relevance and use.	No exceptions noted.
		For each critical system, the entity defines and documents what data and information is critical to support the system.	Inspected data classification policy to determine that for each critical system, the entity defined and documented what data and information was critical to support the system.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity has defined the following components of the data critical to supporting the system • A description of what the critical data is and is used for • Source of the data • How the data is stored and transmitted	Inspected data classification policy to determine that the entity defined the following components of the data critical to supporting the system: • A description of what the critical data is and is used for • Source of the data • How the data is stored and transmitted	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 identified for each identified vulnerability	Inspected risk management policy to determine that the entity's risk assessment process included: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the risk assessment matrix to determine that the entity's risk assessment process included: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability	No exceptions noted.

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.	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 policy to determine that changes to the regulatory, economic and physical environment in which the entity operates were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the risk assessment matrix to determine that changes to the regulatory, economic and physical environment in which the entity operates were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the risk assessment matrix to determine that changes to the business structure and operations were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment policy to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the risk assessment matrix to determine that changes in key management and personnel were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
		Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.
			Inspected the risk assessment matrix 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 policy 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.
			Inspected the risk assessment matrix 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.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 has no Business Associate that access ePHI information, all is handled by internal employees and there is row security enable, in which they cannot have access to client data.	Not applicable.	Not applicable.
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 has no Business Associate that access ePHI information, all is handled by internal employees and there is row security enable, in which they cannot have access to client data.	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)(3)	**Written contract or other 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 Organizational Requirements).	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.	Inquired of the Security Engineer regarding business associate agreements to determine that the entity-maintained business associate agreements with businesses that create, receive maintain, or transmit ePHI.	No exceptions noted.
			Inspected the business associate agreements for an example business associate that hand ePHI and vendor management policy to determine that the entity-maintained business associate agreements with businesses that create, receive maintain, or transmit ePHI.	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.	Inquired of the Security Engineer regarding business associate agreements to determine that the entity-maintained business associate agreements with businesses that create, receive maintain, or transmit ePHI.	No exceptions noted.
			Inspected the business associate agreements for an example business associate that hand ePHI and vendor management policy to determine that the entity-maintained business associate agreements with businesses that create, receive maintain, or transmit ePHI.	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.	Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity plan was tested on an annual basis and included: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	No exceptions noted.
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.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 Security Engineer regarding workstation use standards to determine that procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI were in place.	No exceptions noted.
			Inspected the information security policies to determine that procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI were in place.	No exceptions noted.
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)(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 disposal and destruction policies and procedures to determine policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity purges data stored on backup tapes and backup drives, per a defined schedule.	Inquired of the Security Engineer regarding data disposal to determine that the entity purged data stored on backup tapes and backup drives, per a defined schedule.	No exceptions noted.
			Inspected the data disposal and destruction policies and procedures to determine that the entity purged data stored on backup tapes and backup drives, per a defined schedule.	No exceptions noted.
			Inspected the schedule for when to purge data to determine that the entity purged data stored on backup tapes and backup drives, per a defined schedule.	Testing of this control activity disclosed that no data disposal occurred during the review period.
		The entity purges confidential data after it is no longer required to achieve the purpose for which the data was collected and processed.	Inquired of the Security Engineer regarding data disposal to determine that the entity purged confidential data after it no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.
			Inspected the data disposal and destruction policies and procedures to determine that the entity purged confidential data after it no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the service ticket for an example request to dispose of data, purge a system, or physically destroy a system to determine that the entity purged confidential data after it no longer required to achieve the purpose for which the data was collected and processed.	Testing of this control activity disclosed that no data disposal occurred during the review period.
		An inventory log is maintained of assets with confidential data, and as confidential data meets the retention period, the data is destroyed or purged.	Inspected the inventory log to determine that an inventory log was maintained of assets with confidential data, and as confidential data met the retention period, the data was destroyed or purged.	No exceptions noted.
		Policies and procedures are in place for removal of media storing critical data or software.	Inspected the acceptable use policy to determine policies and procedures were in place for removal of media storing critical data or software.	No exceptions noted.
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. 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.	The entity purges confidential data after it is no longer required to achieve the purpose for which the data was collected and processed.	Inquired of the Security Engineer regarding data disposal to determine that the entity purged confidential data after it no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.
			Inspected the data disposal and destruction policies and procedures to determine that the entity purged confidential data after it no longer required to achieve the purpose for which the data was collected and processed.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the service ticket for an example request to dispose of data, purge a system, or physically destroy a system to determine that the entity purged confidential data after it no longer required to achieve the purpose for which the data was collected and processed.	Testing of this control activity disclosed that no data disposal occurred during the review period.
		An inventory log is maintained of assets with confidential data.	Inspected the inventory log to determine that an inventory log was maintained of assets with confidential data.	No exceptions noted.
		Confidential information is protected from erasure or destruction during the specified retention period.	Inspected the confidentiality policies and procedures to determine that confidential information was protected from erasure or destruction during the specified retention period.	No exceptions noted.
164.310 (d)(2)(iii)	**Accountability:** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Procedures are in place to provide for complete, accurate, and timely storage of data.	Inspected the entity's policies and procedures to determine that procedures were in place to provide for complete, accurate, and timely storage of data.	No exceptions noted.
		Part of 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.	The ways in which critical data are backed up and stored are documented and reviewed annually.	Inspected the entity's policies to determine that the ways in which critical data were backed up and stored were documented and reviewed annually.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the entity's policies to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		Full backups of certain application and database components are performed on a weekly.	Inspected the backup schedule and configurations for an example critical system to determine that full backups of certain application and database components were performed on a daily basis and incremental backups were performed on a weekly basis.	No exceptions noted.
			Inspected the backup history logs for a sample of weeks to determine that full backups of certain application and database components were performed on a monthly basis and incremental backups were performed on a monthly basis.	No exceptions noted.
		When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure.	Inspected backup configurations and an example backup alert to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure.	No exceptions noted.
		Data backed up is replicated to an offsite facility in real-time.	Inspected backup replication configurations to determine that data backed up was replicated to an offsite facility real-time.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Control self-assessments that include Backup restoration tests are performed on at least an annual basis.	Inspected the completed backup restoration test to determine that control self-assessments that included Backup restoration tests were performed on at least an annual 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).	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies, the security governance policy, the access control policy and to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Security Engineer regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the hiring procedures, network, operating system, database, application, and VPN user listings, and user access request ticket for a sample of new hire 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**
		Logical access to systems is revoked as a component of the termination process.	Inspected the termination procedures, network, operating system, database, application, and VPN user listings, and user access revocation ticket for an example 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.
164.312 (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 settings, authentication, access, and security monitoring.	Inspected the information security policies, the security governance policy, the access control policy and to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
	Network			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging settings and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding network audit to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
	Operating System - SaaS Environment (Application, Web, and Database Servers)			
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the SaaS environment user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Operating system audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events	Inspected the operating system audit logging settings and example operating system audit log extracts to determine that operating system audit logging configurations were in place that included: • Account logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted.
		Operating system audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding operating system audit logs to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example operating system audit log extract to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
	Database			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database audit logging settings are in place that include: • Account logon events • Logon events • Process tracking • System events	Inspected the database audit logging settings and an example database audit log extract to determine that database audit logging configurations were in place that included: • Account logon events • Logon events • Process tracking • System events	No exceptions noted.
		Database audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding Database audit logs to determine the database audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example database audit log extract to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.
	Application			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the SaaS listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application audit policy settings are in place that include: • Account logon events • Logon events • Process tracking • System events	Inspected the application audit logging settings and an example application audit log extract to determine that application audit logging configurations were in place that included: • Account logon events • Logon events • Process tracking • System events	No exceptions noted.
		Application audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding application audit logs to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example application audit log extract to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
	Remote Access			
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Access into the environment by outside entities requires a valid user ID and password and invalid login attempts are configured to be logged.	Inspected the VPN authentication settings, VPN audit logging configurations and an example audit log extract for VPN access to determine that access into the environment by outside entities required a valid user ID and password and invalid login attempts were configured to be logged.	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.	Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.	Inspected the business continuity and disaster recovery plans to determine that a business continuity plan was documented and in place that outlined the range of disaster scenarios and steps the business would take in a disaster to ensure the timely resumption of critical business operations.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity plan was tested on an annual basis and included: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	No exceptions noted.
		The ways in which critical data are backed up and stored are documented and reviewed annually.	Inspected the disaster recovery policy to determine that the ways in which critical data were backed up and stored were documented and reviewed annually.	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the disaster recovery policy to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		Full backups of certain application and database components are performed on a weekly.	Inspected the backup schedule and configurations for an example critical system to determine that full backups of certain application and database components were performed on a daily basis and incremental backups were performed on a weekly basis.	No exceptions noted.

TECHNICAL 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 weeks to determine that full backups of certain application and database components were performed on a monthly basis and incremental backups were performed on a monthly basis.	No exceptions noted.
		When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure.	Inspected backup configurations and an example backup alert to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure.	No exceptions noted.
		Data backed up is replicated to an offsite facility in real-time.	Inspected backup replication configurations to determine that data backed up was replicated to an offsite facility in real-time.	No exceptions noted.
		Backups of critical data are maintained securely offsite by a third-party.	Inspected the contract with the offsite backup storage vendor to determine that backups of critical data were maintained offsite by a third-party.	No exceptions noted.
			Inspected the attestation report of the backup storage vendor to determine backups of critical data were maintained offsite by a third-party.	No exceptions noted.
		Control self-assessments that include backup restoration tests are performed on at least an annual basis.	Inspected the completed backup restoration test to determine that control self-assessments that included Backup restoration tests were performed on at least an annual 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)(2)(iii)	**Automatic logoff:** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies, the security governance policy, the access control policy and to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
	Network			
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the network account lockout settings to determine that network account lockout settings were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
	Operating System (Application, Web, and Database Servers)			
		Operating system account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Database			
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the database account lockout settings to determine that database account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
	Application			
		Application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the application account lockout settings to determine that application account lockout settings were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
	Remote Access			
		VPN account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the VPN account lockout settings to determine that application account lockout settings were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
164.312 (a)(2)(iv)	**Encryption and decryption:** Implement a mechanism to encrypt and decrypt ePHI.	Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority.	Inspected encryption configurations to determine that server certificate-based authentication was used as part of the SSL 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**
		VPN, SSL and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine VPN, SSL and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Critical data is stored in encrypted format using Advanced Encryption Standard (AES), 3DES, RSA, ECC, DES and Diffe-Hellman.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES, 3DES, RSA, ECC, DES and Diffe-Hellman.	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.	Regular monitoring and review of logins and log-in attempts to the system is in place. Discrepancies and potentially inappropriate or illegal activities are reported to senior management, legal counsel and/or human resources, as appropriate.	Inspected the Logging and Monitoring Policy to determine that regular monitoring and review of logins and log-in attempts to the system was in place. Discrepancies and potentially inappropriate or illegal activities were reported to senior management, legal counsel and/or human resources, as appropriate.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Network			
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging settings and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding network audits logs to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained and reviewed as needed.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Operating System			
		Operating system audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events	Inspected the operating system audit logging settings and example operating system audit log extracts to determine that operating system audit logging configurations were in place that included: • Account logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted.
		Operating system audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding operating system audit logs to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example operating system audit log extract to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
	Database			
		Database audit logging settings are in place that include: • Account logon events • Logon events • Process tracking • System events	Inspected the database audit logging settings and an example database audit log extract to determine that database audit logging configurations were in place that included: • Account logon events • Logon events • Process tracking • System events	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding database audit logs to determine the database audit logs were maintained and reviewed as needed. Inspected an example database audit log extract to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted. No exceptions noted.
	Application			
		Application audit policy settings are in place that include: • Account logon events • Logon events • Process tracking • System events Application audit logs are maintained and reviewed as needed.	Inspected the application audit logging settings and an example application audit log extract to determine that application audit logging configurations were in place that included: • Account logon events • Logon events • Process tracking • System events Inquired of the Security Engineer regarding application audit logs to determine that application audit logs were maintained and reviewed as needed. Inspected an example application audit log extract to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted. No exceptions noted. No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Physical Access			
		The badge access system logs successful and failed physical access attempts. The logs can be pulled for review if necessary.	Not applicable.	Not applicable.
164.312 (c)(1)	**Integrity:** Implement policies and procedures to protect ePHI from improper alteration or destruction.	Data that entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the IDS configurations, IPS configurations, encryption methods and configurations and VPN authentication configurations to determine that data entered into the system, processed by the system and output from the system was protected from unauthorized access.	No exceptions noted.
		File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the FIM configurations to determine FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software, an example log extract from the IDS and an example IDS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the FIM configurations to determine FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 settings, authentication, access, and security monitoring.	Inspected the information security policies, the security governance policy, the access control policy and to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
	Network			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Network administrative access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer regarding Network administrative access to determine that network administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Networks are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length	Inspected the network password settings to determine that networks were configured to enforce password requirements that included: • Password history • Password age (minimum and maximum) • Password length	No exceptions noted.
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the network account lockout settings to determine that network account lockout settings were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Network audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events	Inspected the network audit logging settings and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding network audit logs to determine that network audit logs were maintained and reviewed as 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 reviewed as needed.	No exceptions noted.
	Operating System (Application, Web, and Database Servers)			
		Operating system user access is restricted via role-based security privileges defined within the access control system.	Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Operating system administrative access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer regarding administrative access to determine that operating system administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
			Inspected the operating system administrator listing to determine that operating system administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
		Operating systems are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length	Inspected the operating system password settings to determine that operating systems were configured to enforce password requirements that included: • Password history • Password age (minimum and maximum) • Password length	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Operating system account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Operating system audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events	Inspected the operating system audit logging settings and example operating system audit log extracts to determine that operating system audit logging configurations were in place that included: • Account logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted.
		Operating system audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding operating system audit logs to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example operating system audit log extract to determine that operating system audit logs were maintained and reviewed as needed.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Database			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Database administrative access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer regarding administrative access to determine that database administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
			Inspected the database administrator listing to determine that database administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
		Databases are configured to enforce password requirements that include: • Password history: 0 • Password age: 0 • Password length: 12 minimum • MFA	Inspected the database password settings to determine that database were configured to enforce password requirements that included: • Password history: 0 • Password age: 0 • Password length: 12 minimum • MFA	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the database account lockout settings to determine that database account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Database audit logging settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events	Inspected the database audit logging settings and an example database audit log extract to determine that database audit logging configurations were in place that included: • Account logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted.
		Database audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding database audit logs to determine the database audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example database audit log extract to determine that database audit logs were maintained and reviewed as needed.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Application			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Application administrative access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer, Grant Elliot on February 22, 2023, regarding administrative access to determine that application administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
			Inspected the application administrator listing to determine that application administrative access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
		The application is configured to enforce password requirements that include: • Password history • Password age (minimum) • Password length	Inspected the application password settings to determine that application was configured to enforce password requirements that included: • Password history • Password age (minimum) • Password length	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 settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the application account lockout settings to determine that application account lockout settings were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Application audit policy settings are in place that include: • Account logon events • Object access • Policy changes • Process tracking • System events	Inspected the application audit logging settings and an example database audit log extract to determine that application audit logging configurations were in place that included: • Account logon events • Object access • Policy changes • Process tracking • System events	No exceptions noted.
		Application audit logs are maintained and reviewed as needed.	Inquired of the Security Engineer regarding Application audit logs to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected an example application audit log extract to determine that application audit logs were maintained and reviewed as needed.	No exceptions noted.
	Remote Access			
		VPN user access is restricted via role-based security privileges defined within the access control system.	Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The ability to administer VPN access is restricted to user accounts accessible by appropriate and authorized personnel.	Inquired of the Security Engineer regarding administrative access to determine that the ability to administer VPN access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
			Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to user accounts accessible by appropriate and authorized personnel.	No exceptions noted.
		VPN users are authenticated via multi-factor authentication (username, password, and PIN/OTP/Token) prior to being granted remote access to the system.	Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
		Access into the environment by outside entities requires a valid user ID and password and invalid login attempts are configured to be logged.	Inspected the VPN authentication settings, VPN audit logging configurations and an example audit log extract for VPN access to determine that access into the environment by outside entities required a valid user ID and password and invalid login attempts were configured to be logged.	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.	Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority.	Inspected encryption configurations to determine that server certificate-based authentication was used as part of the SSL 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**
		VPN, SSL and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine VPN, SSL and other encryption technologies were used for defined points of connectivity.	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.
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.	Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority.	Inspected encryption configurations to determine that server certificate-based authentication was used as part of the SSL encryption with a trusted certificate authority.	No exceptions noted.
		VPN, SSL and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine VPN, SSL and other encryption technologies were used for defined points of connectivity.	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.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software, an example log extract from the IDS and an example IDS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment.	Inspected the FIM configurations to determine FIM software was in place to ensure only authorized changes are deployed into the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the FIM configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.312 (e)(2)(ii)	**Encryption:** Implement a mechanism to encrypt ePHI whenever deemed appropriate.	Server certificate-based authentication is used as part of the SSL encryption with a trusted certificate authority.	Inspected encryption configurations to determine that server certificate-based authentication was used as part of the SSL encryption with a trusted certificate authority.	No exceptions noted.
		VPN, SSL and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine VPN, SSL and other encryption technologies were used for defined points of connectivity.	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.
		Critical data is stored in encrypted format using AES, 3DES, RSA, ECC, DES and Diffe-Hellman.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES, 3DES, RSA, ECC, DES and Diffe-Hellman.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected the encryption configurations for an example backup media to determine that backup media was stored in an encrypted format.	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."	Not applicable. The entity has no Business Associate that access ePHI information, all is handled by internal employees and there is row security enable, in which they cannot have access to client data.	Not applicable.	Not applicable.
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."	Not applicable. The entity has no Business Associate that access ePHI information, all is handled by internal employees and there is row security enable, in which they cannot have access to client data.	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 (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.	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 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**
164.316 (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.	Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.	Inspected the entity policies and procedures to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
			Inspected meeting Modules to determined that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
		Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's, intranet.	Inspected the information security policies and procedures, a sample of job description and the entity's intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.	No exceptions noted.
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.	Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.	Inspected the entity policies and procedures to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
			Inspected meeting Modules to determined that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.	Inspected the information security policies and procedures, a sample of job description and the entity's intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's Intranet.	No exceptions noted.
164.316 (b)(1)(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.	The entity retains all documentation for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect.	Inquired of the Inquired of the Security Engineer regarding documentation retention standards to determine that the entity retained documentation for a minimum period of six (6) years from the date of creation or modification, or the date when it was last in effect.	No exceptions noted.
			Inspected the HIPAA documentation retention policy to determine that the entity retained documentation for a minimum period of six (6) years from the date of creation or modification, or the date when it was last in effect.	No exceptions noted.
164.316 (b)(1)(ii)	**Availability:** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.	Inspected the information security policies and procedures, a sample job description and the entity's intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet.	No exceptions noted.

ORGANIZATIONAL REQUIREMENTS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.316 (b)(1)(ii)	**Updates:** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.	Inspected the entity policies and procedures to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis. Inspected meeting Modules to determined that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted. 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 Inquired of the 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	

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the breach notification 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 an example breach 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 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)(1)	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 (a)(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.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 • 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 Inquired of the 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	

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the breach notification 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 an example breach 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 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 Inquired of the 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 breach notification policy 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 an example breach 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 this control activity disclosed that no breaches 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 Inquired of the 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 breach notification policy 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 an example breach 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 this control activity disclosed that no breaches 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 who's unsecured ePHI has been accessed during the breach is disclosed during notification procedures.	Inquired of the Inquired of the Security Engineer regarding known breaches of ePHI to determine that the identification of each individual who's unsecured ePHI has been accessed during the breach was disclosed during notification procedures.	No exceptions noted.
			Inspected the breach notification policy to determine that procedures were in place to guide personnel in disclosing the identification of each individual who's unsecured ePHI was accessed during the breach.	No exceptions noted.
			Inspected an example breach of ePHI to determine that the identification of each individual who's unsecured ePHI has been accessed during the breach was disclosed during notification procedures.	Testing of this control activity disclosed that no breaches 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 (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 Inquired of the 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 breach notification policy 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 an example breach 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. notification procedures.	Testing of this control activity disclosed that no breaches 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 HHS HIPAA investigations policy and the HIPAA state law preemption policy 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.
164.414	**Administrative requirements and burden of proof**: 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 HHS HIPAA investigations policy 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
CC1.1, CC1.4, CC1.5	Performance evaluations are performed for personnel on an annual basis.	Inspected the performance evaluation form for a sample of current employees to determine that performance evaluations were performed for personnel on an annual basis.	Testing of the control activity disclosed that performance evaluation was not formally complete for seven of the twelve current employees sampled.	Profisee acknowledges the findings in these exceptions and is currently working to reform processes, procedures, and documentation to better refine these processes and make improvements in procedure.
CC1.2	Executive management evaluates the skills and competencies of those that operate the internal controls within the environment annually.	Inspected the performance 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.	Testing of the control activity disclosed that performance evaluation was not formally complete for seven of the twelve current employees sampled.	Profisee acknowledges the findings in these exceptions and is currently working to reform processes, procedures, and documentation to better refine these processes and make improvements in procedure.
CC4.1	Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance evaluation form for a sample of current employees to determine that performance evaluations were performed for personnel on an annual basis.	Testing of the control activity disclosed that performance evaluation was not formally complete for seven of the twelve current employees sampled.	Profisee acknowledges the findings in these exceptions and is currently working to reform processes, procedures, and documentation to better refine these processes and make improvements in procedure.