A-LIGN

A-LIGN.com

Type 2 SOC 2 with HIPAA/HITECH

Prepared for:
Springs Hosting

Year:
2025

Springs Hosting

FRONTIERIT
TECHNOLOGY THAT FITS

REPORT ON SPRINGS HOSTING'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

July 1, 2024 to June 30, 2025

Table of Contents

SECTION 1

ASSERTION OF SPRINGS HOSTING MANAGEMENT

ASSERTION OF SPRINGS HOSTING MANAGEMENT

September 17, 2025

We have prepared the accompanying description of Springs Hosting's (or 'the Company') Colocation and Managed Services titled "Springs Hosting's Description of Its Colocation and Managed Services throughout the period July 1, 2024 to June 30, 2025" (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 Colocation and Managed Services that may be useful when assessing the risks arising from interactions with Springs Hosting's system, particularly information about system controls that Springs Hosting 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.

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

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

a. the description presents Springs Hosting's Colocation and Managed Services that was designed and implemented throughout the period July 1, 2024 to June 30, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Springs Hosting'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 user entities applied the complementary controls assumed in the design of Springs Hosting's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Springs Hosting's service commitments and system requirements were achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, if complementary user entity controls assumed in the design of Springs Hosting's controls operated effectively throughout that period.

Kelly Karnetsky

Kelly Karnetsky
CEO
Springs Hosting

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Springs Hosting

Scope

We have examined Springs Hosting's accompanying description of its Colocation and Managed Services titled "Springs Hosting's Description of Its Colocation and Managed Services throughout the period July 1, 2024 to June 30, 2025" (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 July 1, 2024 to June 30, 2025, to provide reasonable assurance that Springs Hosting'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.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Springs Hosting, to achieve Springs Hosting's service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Springs Hosting's controls, the applicable trust services criteria, HIPAA/HITECH requirements, and the complementary user entity controls assumed in the design of Springs Hosting'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 Springs Hosting Service Organization That Is Not Covered by the Service Auditor's Report," is presented by Springs Hosting management to provide additional information and is not a part of the description. Information about Springs Hosting'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 Springs Hosting's service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements.

Service Organization's Responsibilities

Springs Hosting 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 Springs Hosting's service commitments and system requirements were achieved. Springs Hosting has provided the accompanying assertion titled "Assertion of Springs Hosting Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Springs Hosting 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 Springs Hosting's Colocation and Managed Services that was designed and implemented throughout the period July 1, 2024 to June 30, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Springs Hosting'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 user entities applied the complementary controls assumed in the design of Springs Hosting's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Springs Hosting's service commitments and system requirements were achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, if complementary user entity controls assumed in the design of Springs Hosting'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 Springs Hosting, user entities of Springs Hosting's Colocation and Managed Services during some or all of the period July 1, 2024 to June 30, 2025, business partners of Springs Hosting subject to risks arising from interactions with the Colocation and Managed Services, 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, and other parties
- Internal control and its limitations
- Complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria and HIPAA/HITECH requirements
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

A-LIGN ASSURANCE

Tampa, Florida
September 17, 2025

SECTION 3

SPRINGS HOSTING'S DESCRIPTION OF ITS COLOCATION AND MANAGED SERVICES SYSTEM THROUGHOUT THE PERIOD JULY 1, 2024 TO JUNE 30, 2025

OVERVIEW OF OPERATIONS

Company Background

Springs Hosting is a leading Hosting Service Provider (HSP) and Data Center headquartered in Colorado Springs, Colorado. Springs Hosting boasts an extensive list of certifications to meet customer requirements that include SSAE18 Type II Compliant, Health Insurance Portability and Accountability Act (HIPAA) Compliant, Payment Card Industry (PCI) Compliant, and UL Listed (UL827). Since 2006, Springs Hosting has been providing customers with managed services that include colocation, Internet service provider, cloud services provider, Disaster Recovery As A Service (DRAAS), website and email hosting. Customers trust their critical data systems to Springs Hosting for meeting today’s ever evolving reliability and commitment workplace challenges.

In January 2016, Springs Hosting launched Frontier IT and transitioned the related Managed Service Provider (MSP). Customers continue to receive the same support with which they are already familiar. Springs Hosting will continue to provide customers with data centers and managed hosting services under the existing brand.

Frontier IT provides a large technical capacity in the industry delivering critical Information Technology (IT) business services to customers.

Description of Services Provided

Consulting services include:

- Best Practices for Server and Network Architecture and Support
- Best Practices for Disaster Recovery and how-to backup properly
- Business Phone Systems
- Microsoft Office 365
- Obtaining and maintaining HIPAA compliance
- Efficiently using cloud services

Helpdesk services include:

- Fixed fee monthly cost
- Access to the virtual Chief Information Officer (vCIO) team forecasting future requirements
- 24/7 network monitoring
- Antivirus and malware updates and protection
- Server and network maintenance
- Hardware provisioning and deployment
- Onsite and remote support

Workplace file synchronization and sharing solution:

- Support for Multiple Devices
- Cross-Device Collaboration and Editing
- Smart Sync Capabilities
- On and Offline Access
- Version Control
- Secure Sharing without Forced Registration
- Scan to PDF for Instant Field Image and Document Capture
- Automated Document Quick Response (QR) Coding
- Encryption In-session, In-transit, On-device
- Policy-based Control of Content, Users and Devices
- Download / Copy Prevention, Auto PDF
- Built-in Remote Wipe Capabilities
- Two-factor Authentication

- Share Content with Links
- Inactivity Session Timers
- Internet Protocol (IP) Address Whitelisting
- Systems Integration
- Real-time, Multi-Platform Sync
- No File Size Limit
- Continuous Real-time Backup
- Cloud-enable Your File Server

Principal Service Commitments and System Requirements

Springs Hosting designs its processes and procedures related to Colocation and Managed Services to meet its objectives for its Colocation and Managed Services. Those objectives are based on the service commitments that Springs Hosting makes to user entities, the laws and regulations that govern the provision of Colocation and Managed Services, and the financial, operational, and compliance requirements that Springs Hosting has established for the services. The Colocation and Managed Services of Springs Hosting are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Springs Hosting operates.

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

- Security principles within the fundamental designs of the Colocation and Managed Services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect data both at rest and in transit, such as transport layer security (TLS) and advanced encryption standards (AES)

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

Components of the System

Infrastructure

Primary infrastructure used to provide Springs Hosting’s Colocation and Managed Services includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Cisco Stack (Core)	Switch Stack	Connects primary devices in the network
Cisco Meraki	Firewall	Prevent unauthorized access to the network

Software

Primary software used to provide Springs Hosting's Colocation and Managed Services includes the following:

Primary Software	
Software	**Purpose**
Autotask PSA	Ticket System, Incident logging, tracking and review application
Datto Endpoint Management	Remote Monitoring and Management
Meraki	Cloud Network
Office 365	Operating system to run Microsoft Outlook, OneDrive, and Microsoft applications
Datto Workplace	File Sharing application
WHMCS	Hosting Ticket and Billing System

People

Springs Hosting has a staff of approximately 11 employees organized in the following functional areas:

- *Corporate*. Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, human resources. These individuals use the Colocation and Managed Services primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics, audit support, and service quality management.
- *IT.* Personnel responsible for help desk support, IT infrastructure, networking, systems administration, software systems management, information security, and IT operations. These groups collectively manage electronic interfaces, system reliability, and service delivery for the Colocation and Managed Services:
    - The help desk group provides technical assistance to the Colocation and Managed Services users.
    - The infrastructure, networking, and systems administration staff maintain Springs Hosting's IT infrastructure, which supports the Colocation and Managed Services. A systems administrator deploys releases of the Colocation and Managed Services and other related software into production environments.
    - The software and systems management staff maintain internal and client-facing systems used to support the Colocation and Managed Services, including the management of applications, utilities, and integrations. The information security staff supports the Colocation and Managed Services indirectly by monitoring internal and external security threats and maintaining current antivirus software.
    - The information security staff maintains the inventory of IT assets.
    - The IT operations staff manage user interfaces for the Colocation and Managed Services and ensure operational continuity of core hosting, monitoring, and backup services. Telecom personnel maintain the voice communications environment, provide user support to Springs Hosting, and resolve communication problems. This group does not directly use the Colocation and Managed Services, but it provides infrastructure support as well as disaster recovery assistance.

Data

Data, as defined by Springs Hosting, constitutes the following:

- Client account data and configuration files
- Transaction and system event data

- System reports and usage logs
- Input and configuration records
- System files and infrastructure metadata
- Error logs and audit trails

Transaction processing within the Colocation and Managed Services is initiated by service requests, monitoring events, or scheduled system activities. Requests are logged through ticketing, automation, or monitoring systems and processed by authorized personnel according to established change-control and service-delivery procedures.

All client data, configuration changes, and system activities are recorded electronically within Springs Hosting's management platforms (Autotask PSA, Datto RMM, WHMCS, and related systems). Manual data entry is limited to approved administrative tasks.

Output reports are available in electronic PDF, comma-delimited value file exports, or electronically from the various websites. The availability of these reports is limited by job function. Reports delivered externally will only be sent using a secure method-encrypted email, secure FTP, or secure websites-to transportation providers, treating facilities, and governments or managed care providers using Springs Hosting-developed websites or over connections secured by trusted security certificates. Springs Hosting uses TLS to encrypt email exchanges with government or managed care providers, facility providers, and transportation providers.

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 the Springs Hosting policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Springs Hosting team member.

<u>Physical Security</u>

Wholly occupied company facilities are protected by walls and fencing around the entire perimeter. Each facility has a designated reception area which is attended by either a receptionist or a security guard. Access to the reception area is unlocked from 8am to 5pm on business days and is locked at all other times. When locked, a visitor presses a buzzer to attract the attention of the guard at the visitor desk who can release the lock. The door may also be unlocked through the use of an access card/ID that has been assigned general access to the facility. Access beyond the reception area is controlled through the access card system.

All remaining exterior ingress doors are restricted to users possessing an access card/ID that has been assigned access to use the door. The access card/ID system uses zones to control access. Each exterior door and doors to restricted areas within the facilities are assigned to door zones. Access to zones is restricted through the use of access control lists. Employees and vendors granted access cards are assigned to roles based on their job responsibilities.

Visitors check in with the receptionist or security guard stationed in the reception area. Visitors ought to present a valid, government-issued photo ID. The visitor's name, employer, and purpose for visit are recorded in a visitor log and his or her visit ought to be approved by a Springs Hosting employee who is authorized to sign non-employees into the facility. The visitor is issued a temporary ID badge to be worn throughout his or her visit. This temporary badge does not permit users access through any secured doors within the facility.

Entrances to data centers are restricted by two doors; access through the first door is gained by using a key card to deactivate the locking mechanism, and access through the second door is granted by using a biometric hand reader and personal identification number (PIN).

Upon an employee's termination of employment, the HR system automatically generates an access deletion record in the event management system on the last day of employment. This record is routed to the access administrators for deletion. In addition, terminated employees turn over their access cards/IDs during their exit interview. These cards are then sent via interoffice mail to physical security for recording and destruction.

On an annual basis, the director of physical security sends a list of each vendor's employees who have been granted access to the vendor contact to review appropriateness of employee access. Vendors are required to return the confirmation of access within two weeks. The director follows up on any access lists not returned.

Logical Access

Springs Hosting uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, Springs Hosting implements monitoring of one or more of the responsibilities. Monitoring ought to be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

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

Upon hire, employees are assigned to a position in the HR management system. Two days prior to the employees' start date, the HR management system creates a report of employee user IDs to be created and access to be granted. The report is used by the security help desk to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

On an annual basis, access rules for each role are reviewed by a working group composed of security help desk, data center, customer service, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the CISO. As part of this process, the CISO reviews access by privileged roles and requests modifications based on this review.

The HR system generates a list of terminated employees. This report is used by the security help desk to delete employee access. On an annual basis, HR runs a list of active employees. The security help desk uses this list to suspend user IDs and delete all access roles from IDs belonging to terminated employees.

Computer Operations - Backups

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

Backup infrastructure are physically secured in locked cabinets and/or caged environments within the third-party data centers. The backup infrastructure resides on private networks logically secured from other networks.

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.

Springs Hosting monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Springs Hosting evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space, power and cooling
- Disk storage
- Network bandwidth

Change Control

Springs Hosting maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new infrastructure changes. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

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

Data Communications

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

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

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

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

Boundaries of the System

The scope of this report includes the Colocation and Managed Services performed in the Colorado Springs, Colorado facility.

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

Control Environment

Integrity and Ethical Values

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

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

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

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

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

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

Management's Philosophy and Operating Style

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

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

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

Organizational Structure and Assignment of Authority and Responsibility

Springs Hosting'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.

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

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

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.\

Human Resource Policies and Practices

Springs Hosting's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Springs Hosting'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.

Risk Assessment Process

Springs Hosting’s risk assessment process identifies and manages risks that could potentially affect Springs Hosting’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. Springs Hosting 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 Springs Hosting, 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

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

Integration with Risk Assessment

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

Information and Communications Systems

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

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

Specific information systems used to support Springs Hosting's Colocation and Managed Services are described in the Description of Services section above.

Monitoring Controls

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

On-Going Monitoring

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

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

Reporting Deficiencies

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

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Periodic Assessments

Springs Hosting 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 Springs Hosting 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) at annual 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 CEO. 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 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 Springs Hosting 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

Springs Hosting 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. Additionally, employees are also required to participate in annual security awareness training.

Periodic Testing and Evaluation

Springs Hosting 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 Springs Hosting'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

Springs Hosting 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 in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

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

The following HIPAA/HITECH requirements were not applicable to the system:

Requirements Not Applicable to the System		
Safeguard	**Requirement**	**Reason**
Administrative Safeguard	164.308(a)(4)(ii)(A)	Not Applicable. The entity is not a healthcare clearinghouse.
Physical Safeguard	164.310(c)	Not Applicable. The entity is not a covered entity.
Organizational Safeguard	164.314(a)(2)(ii)	Not Applicable. The entity is not a government entity.
	164.314(b)(1)	Not Applicable. The entity is not a plan sponsor.
	164.314(b)(2)	Not Applicable. The entity is not a group health plan.
Breach Safeguard	164.404(a)(1), 164.404(a)(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)	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

Subservice Organizations

No subservice organizations were included in the scope of this assessment.

COMPLEMENTARY USER ENTITY CONTROLS

Springs Hosting’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 and HIPAA/HITECH requirements related to Springs Hosting’s services to be solely achieved by Springs Hosting control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Springs Hosting’s.

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

1. User entities are responsible for understanding and complying with their contractual obligations to Springs Hosting.
2. User entities are responsible for notifying Springs Hosting of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Springs Hosting services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Springs Hosting services.
6. User entities are responsible for providing Springs Hosting with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Springs Hosting of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

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.

HEALTH INFORMATION SECURITY PROGRAM

Springs Hosting has developed a health information security management program to meet the information security and compliance requirements related to Colocation and Managed 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 Springs Hosting 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 how Springs Hosting complies with the act:

- Management has adopted a written set of health information security policies and designated the information security officer to be responsible for developing and implementing the required policies and procedures.
- Procedures address access authorization, establishment, modification, and termination.
- Documented incident response policies for reporting security incidents are in place to guide employees in identifying, reporting, of security incidents.
- Business continuity plans are documented to enable continuation of critical business processes in the event of an emergency.

- Privileged administrative access to systems is restricted to authorized individuals.
- Automated backup systems are in place to perform scheduled replication of production data and systems at pre-defined intervals.
- Antivirus software is utilized to detect and eliminate data or files that contain certain virus signatures on certain production servers.

Physical Safeguards - Controlling physical access to protected data:

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

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

- Access to in-scope systems are 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 regards to PHI documentation availability, as well as documentation retention:

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

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

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

Control Activities Specified by the Service Organization

The applicable trust criteria and HIPAA/HITECH requirements, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust criteria and HIPAA/HITECH requirements and related control activities are included in Section 4, they are, nevertheless, an integral part of Springs Hosting's description of the system. Any applicable trust services criteria or HIPAA/HITECH requirements that are not addressed by control activities at Springs Hosting are described within Section 4 and within the Subservice Organization and Criteria Not Applicable to the System sections above.

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

SECTION 4

TRUST SERVICES CATEGORY, CRITERIA, 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 Springs Hosting was limited to the Trust Services Criteria and HIPAA/HITECH requirements, related criteria and control activities specified by the management of Springs Hosting and did not encompass all aspects of Springs Hosting'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, procedures, the code of conduct and the employee handbook.	Inspected the employee handbook, information security policies and procedures and the entity's intranet to determine that core values were communicated from executive management to personnel through policies, procedures, the code of conduct and the employee handbook.	No exceptions noted.
		An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inquired of the CEO regarding the process for new hires to acknowledge the employee handbook and code of conduct to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the employee handbook and code of conduct documentation for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Prior to employment, personnel are required to complete a background check.	Inspected the completed background check form for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inquired of the CEO regarding performance evaluations to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
			Inspected the employee handbook to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
			Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	Testing of the control activities disclosed that performance evaluations were not performed for five of five 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
		Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the company handbook to determine that sanction policies, which included probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.
		A reporting forum is in place to allow employees, third parties, and customers to report unethical behavior in a confidential manner.	Inspected the company reporting forum to determine that a reporting forum was in place to allow employees, third parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
		Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the employee handbook and the entity's website to determine that employees, third parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		Upon hire, personnel are required to sign a confidentiality agreement.	Inspected the employee handbook, which includes the confidentiality agreement, for a sample new hires to determine that upon hire, personnel were required to sign a confidentiality agreement.	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 dates 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.	Inquired of the CEO regarding the process for evaluating the skills and expertise of its members to determine that executive management evaluates the skills and expertise of its members annually.	No exceptions noted.
			Inspected the performance evaluation meeting for a sample 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 implemented within the environment.	Inspected the organizational chart and the internal controls matrix to determine that executive management maintained independence from those that operate the key controls implemented within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management meeting invite and emails to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the internal controls matrix and management meeting invite and emails to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.	Inspected the organizational chart and job descriptions and determined that responsible parties were defined and assigned to coordinate and monitor risk management, compliance and audit activities.	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.	Executive management maintains independence from those that operate the key controls implemented within the environment.	Inspected the organizational chart and the internal controls matrix to determine that executive management maintained independence from those that operate the key controls implemented 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 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.
		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.
		Executive management has established proper segregations of duties for key job functions and roles within the organization.	Inspected the organizational chart, the internal controls matrix, and job description for a sample of job roles to determine that executive management established proper segregations of duties for key job functions and roles within the organization.	No exceptions noted.

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**
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	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.
		Prior to employment, personnel are required to complete a background check.	Inspected the completed background check form for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inquired of the CEO regarding performance evaluations to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
			Inspected the employee handbook to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
			Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	Testing of the control activities disclosed that performance evaluations were not performed for five of five 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**
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee handbook and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		The entity evaluates the competencies and experience of candidates prior to hiring.	Inquired of the CEO regarding the process for evaluating the competencies and experience of candidates prior to hiring to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	No exceptions noted.
			Inspected the resume for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	No exceptions noted.
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.	Inquired of the CEO regarding the job requirements documented in the job descriptions and the evaluation of candidates' abilities to meet these requirements as part of the hiring process to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring process.	No exceptions noted.

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 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 were evaluated as part of the hiring process.	No exceptions noted.
		The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives.	Inspected the recruiting policies and procedures and organizational chart job opening postings to determine that the entity had a recruiting department that was responsible for attracting individuals with competencies and experience that aligned with the entity's goals and objectives.	No exceptions noted.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the security and awareness training policy to determine that employees were required to attend continued training annually that related to their job role and responsibilities.	No exceptions noted.
		Executive management has created a training program for its employees.	Inspected the information security and awareness training program to determine that executive management had created a training program for its employees.	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.	Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inquired of the CEO regarding the process for new hires to acknowledge the employee handbook and code of conduct to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the employee handbook and code of conduct documentation for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inquired of the CEO regarding performance evaluations to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
			Inspected the employee handbook to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	Testing of the control activities disclosed that performance evaluations were not performed for five of five current employees sampled.
		Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the company handbook to determine that sanction policies, which included probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.
		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.
		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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee handbook and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		Executive management has established performance measures, including the incentives and rewards for exceeding expectations, as it relates to job roles and responsibilities.	Inspected the employee 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.
		Executive management reviews the job requirements and responsibilities documented within job descriptions annually and makes updates, if necessary.	Inspected the job description including the revision date for a sample of job roles to determine that executive management reviewed the job requirements and responsibilities documented within job descriptions annually and made updates, if necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet.	Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's intranet.	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 the data flow diagram 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.
		Data entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the intrusion detection system (IDS) configurations, intrusion 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Core values are communicated from executive management to personnel through policies, procedures, the code of conduct and the employee handbook.	Inspected the employee handbook, information security policies and procedures and the entity's intranet to determine that core values were communicated from executive management to personnel through policies, procedures, the code of conduct and the employee handbook.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inquired of the CEO regarding the process for new hires to acknowledge the employee handbook and code of conduct to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the employee handbook and code of conduct documentation for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct 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**
		A reporting forum is in place to allow employees, third parties, and customers to report unethical behavior in a confidential manner.	Inspected the company reporting forum to determine that a reporting forum was in place to allow employees, third parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
		Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the employee handbook and the entity's website to determine that employees, third parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		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.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the security and awareness training policy to determine that employees were required to attend continued training annually that related to their job role and responsibilities.	No exceptions noted.
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet.	Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to 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, code of conduct and employee handbook are made available to personnel through the entity's intranet.	Inquired of the CEO regarding entity intranet to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to personnel through the entity's intranet.	No exceptions noted.
			Observed the entity's intranet to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to personnel through the entity's intranet.	No exceptions noted.
			Inspected the entity's intranet to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to personnel through the entity's intranet.	No exceptions noted.
		Upon hire, personnel are required to complete information security awareness training.	Inspected the information security awareness training completion tracking tool for a sample of new hires to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
		Current employees are required to complete information security awareness training annually.	Inspected the information security awareness training completion tracking tool for a sample of current employees to determine that current employees were required to complete information security awareness training annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the management meeting invite and emails 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.
		Changes to job roles and responsibilities are communicated to personnel through the entity's intranet.	Inspected the 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 system failures, incidents, concerns, and other complaints are in place and made available to personnel through the entity’s intranet.	Inspected the incident response policies and procedures and the entity’s intranet to determine that documented escalation procedures for reporting system failures, incidents, concerns, and other complaints were in place and made available to personnel 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.
		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 information security policies and procedures to determine that the information security policies and procedures that communicated the system commitments and requirements of external users were provided to external users prior to allowing them access to 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
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.	Inspected the organizational chart and job descriptions and determined that responsible parties were defined and assigned to coordinate and monitor risk management, compliance and audit activities.	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.	Inquired of the CEO regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
			Inspected the information security policy regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	A reporting forum is in place to allow employees, third parties, and customers to report unethical behavior in a confidential manner.	Inspected the company reporting forum to determine that a reporting forum was in place to allow employees, third parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
		Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the employee handbook and the entity's website to determine that employees, third parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place and made available to personnel through the entity’s intranet.	Inspected the incident response policies and procedures and the entity’s intranet to determine that documented escalation procedures for reporting system failures, incidents, concerns, and other complaints were in place and made available to personnel through the entity's intranet.	No exceptions noted.
		The entity's third-party agreement delineates the boundaries of the system and describes relevant system components.	Inspected the third-party agreement for a sample of third parties to determine that the entity’s third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The entity's third-party agreement communicates the system commitments and requirements of third parties.	Inspected the third-party agreement for a sample of third parties to determine that the entity's third-party agreement communicated the system commitments and requirements of third parties.	No exceptions noted.
		The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third parties.	Inspected the third-party agreement for a sample of third parties to determine that the entity's third-party agreement outlined and communicated the terms, conditions and responsibilities of third parties.	No exceptions noted.
		The entity's contractor agreement outlines and communicates the terms, conditions and responsibilities of external users.	Inspected the contractor agreement template to determine that the entity's contractor agreement outlined and communicated the terms, conditions and responsibilities of external users.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the customer agreement template and customer agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
		Changes to commitments, requirements and responsibilities are communicated to third parties, external users, and customers via mass notifications.	Inspected the entity's website to determine that changes to commitments, requirements and responsibilities were communicated to third parties, external users and customers via mass notifications.	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 management meeting invites and emails to determine that executive management met annually with operational management to discuss the results of assessments performed by third parties.	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.	Inquired of the CEO regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
			Inspected the information security policy regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
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.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management meeting invite and emails to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		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.
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet.	Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's intranet.	No exceptions noted.
		The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.	Inspected the organizational chart, employee handbook 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART).	Inspected the entity's documented objectives and strategies to determine that executive management had documented objectives that were SMART.	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
		Executive management reviews policies, procedures and other control documents for alignment to the entity's objectives on an annual basis.	Inspected the management meeting invite, management reports, and emails to determine that executive management reviewed policies, procedures and other control documents for alignment to the entity's objectives on an annual basis.	No exceptions noted.
		Executive management reviews and addresses repeated control failures.	Inquired of the CEO regarding the process for escalating and addressing repeated control failures to determine that executive management reviewed and addressed repeated control failures.	No exceptions noted.
			Inspected the information security policies and management meeting minutes to determine that executive management reviewed and addressed repeated control failures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.	Inspected the organizational chart and job descriptions and determined that responsible parties were defined and assigned to coordinate and monitor risk management, compliance and audit activities.	No exceptions noted.
		The entity has defined the desired level of performance and operation in order to achieve the established entity objectives.	Inspected the 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.

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, the entity's documented objectives and strategies and the documented key performance indicators for operational and internal controls effectiveness to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies.	No exceptions noted.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the entity's budget and documented objectives and strategies to determine that business budgets aligned with the entity's strategies and objectives.	No exceptions noted.
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected the management reports to determine that entity strategies, objectives and budgets were assessed on an annual basis.	No exceptions noted.
		The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures.	Inspected the internal controls matrix, 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 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**
		Applicable law, regulation, standard and legislature requirements are identified and integrated into the entity's strategies and objectives.	Inspected the entity's documented objectives and strategies, 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.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the security management process policy to determine that management had defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on at least 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
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.	Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the documented security management process and the completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment 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.
		Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the documented security management process to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the security management process policy to determine that management had defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.

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

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

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
		For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
		Annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.
		As part of annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third parties.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that as part of annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third parties to evaluate the effectiveness of controls within the vendor or third party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third parties to evaluate the effectiveness of controls within the vendor or third party's environment.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the security management process policy to determine that management had defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on at least 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**
		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 completed fraud assessment to determine that, on an annual basis, management identified and assessed the types of fraud that could impact their business and operations.	No exceptions noted.
		Identified fraud risks are reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the completed fraud assessment to determine that identified fraud risks were reviewed and addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	Inspected the completed fraud assessment to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities.	Inspected the completed fraud assessment to determine that as part of management's assessment of fraud risks, management considered how personnel could engage in or justify fraudulent activities.	No exceptions noted.

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 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).	Inspected the completed fraud assessment to determine that as part of management's assessment of fraud risks, management considered threats and vulnerabilities that arise from the use of IT.	No exceptions noted.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management meeting invite and emails to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment 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.
		Changes to the regulatory, economic and physical environment in which the entity operates are considered and evaluated as part of annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that changes to the regulatory, economic and physical environment in which the entity operates were considered and evaluated as part of annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Changes to the business structure and operations are considered and evaluated as part of annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that changes to the business structure and operations were considered and evaluated as part of annual comprehensive risk assessment.	No exceptions noted.
		Changes in key management and personnel are considered and evaluated as part of annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that changes in key management and personnel were considered and evaluated as part of annual comprehensive risk assessment.	No exceptions noted.
		Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of annual comprehensive risk assessment.	No exceptions noted.
		Changes in vendor and third-party relationships are considered and evaluated as part of annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that changes in vendor and third-party relationships were considered and evaluated as part of 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
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third parties to evaluate the effectiveness of controls within the vendor or third party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third parties to evaluate the effectiveness of controls within the vendor or third party's environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.	Performance and conduct evaluations are performed for personnel on an annual basis.	Inquired of the CEO regarding performance evaluations to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
			Inspected the employee handbook to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
			Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	Testing of the control activities disclosed that performance evaluations were not performed for five of five current employees sampled.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management meeting invite and emails to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment 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.

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**
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet.	Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's intranet.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.	Inspected the organizational chart and job descriptions and determined that responsible parties were defined and assigned to coordinate and monitor risk management, compliance and audit activities.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		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 centralized antivirus software configurations, the IDS configurations, the IPS configurations, and the firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		On an annual basis, management reviews the controls implemented within the environment for compliance and operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the management meeting invite, emails, and internal audit results to determine that on an annual basis, management reviewed the controls implemented within the environment for compliance and operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.
		A data backup restoration test is performed on an annual basis.	Inquired of the CEO regarding restoration testing to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Internal vulnerability scans are performed annually and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results report to determine that internal vulnerability scans were performed annually and remedial actions were taken where necessary.	No exceptions noted.
		A third party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the network and infrastructure security policy to determine that a third party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third parties to evaluate the effectiveness of controls within the vendor or third party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third parties to evaluate the effectiveness of controls within the vendor or third party's environment.	No exceptions noted.
		Logical access reviews are performed annually.	Inquired of the CEO regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the information security policy for the in-scope systems regarding user access reviews to determine that logical access reviews were performed 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 completed access review for the in-scope systems to determine that logical access reviews were performed annually.	Testing of the control activities disclosed that logical access reviews were not performed within the review period. Subsequent testing disclosed that logical access reviews were performed after the review period.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and an example alert notification, and the IDS and IPS configurations and an example alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds had been exceeded.	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.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management meeting invite and emails to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.	Inspected the organizational chart and job descriptions and determined that responsible parties were defined and assigned to coordinate and monitor risk management, compliance and audit activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the documented security management process and the completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		Annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.
		Senior management assesses the results of the compliance, control and risk assessments performed on the environment.	Inspected the management meeting invite and emails 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 the management meeting invite and emails 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 failures/gaps identified from the various assessments performed on the environment are communicated to those parties responsible for taking corrective actions.	Inquired of the CEO regarding the process of communicating vulnerabilities, deviations, and control failures identified from assessments to responsible parties to determine that vulnerabilities, deviations, and control failures identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the various assessments performed on the environment to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting incident tickets for a sample of vulnerabilities identified from a vulnerability scan to determine that vulnerabilities, deviations and control failures identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are documented, investigated, and addressed.	Inquired of the CEO regarding the vulnerability management process to determine that vulnerabilities, deviations, and control failures identified from the various assessments performed on the environment were documented, investigated, and addressed.	No exceptions noted.
			Inspected the information security policy regarding the vulnerability management process to determine that vulnerabilities, deviations and control failures identified from the various assessments performed on the environment were documented, investigated and addressed.	No exceptions noted.
			Inspected the various assessments performed on the environment and supporting incident tickets for a sample of vulnerabilities identified from a vulnerability scan to determine that vulnerabilities, deviations and control failures identified from the various assessments performed on the environment were documented, investigated and addressed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are addressed by those parties responsible for taking corrective actions.	Inquired of the CEO regarding the remediation process for vulnerabilities identified during penetration testing to determine that vulnerabilities were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the Information Security Policy regarding the remediation process for vulnerabilities identified during penetration testing to determine that vulnerabilities, deviations and control failures identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the various assessments performed on the environment and supporting incident tickets for a sample of vulnerabilities identified from a vulnerability scan to determine that vulnerabilities, deviations and control failures identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management tracks whether vulnerabilities, deviations and control failures/gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the incident management meeting invite, emails, and risk assessment to determine that management tracked whether vulnerabilities, deviations and control failures/gaps identified as part of the evaluations performed were addressed in a timely manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Executive management maintains independence from those that operate the key controls implemented within the environment.	Inspected the organizational chart and the internal controls matrix to determine that executive management maintained independence from those that operate the key controls implemented within the environment.	No exceptions noted.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management meeting invite and emails to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.	Inspected the organizational chart and job descriptions and determined that responsible parties were defined and assigned to coordinate and monitor risk management, compliance and audit activities.	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the documented security management process and the completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	Inspected the completed risk assessment to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	No exceptions noted.
		Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	Inquired of the CEO regarding the process for implementing security controls to mitigate vulnerabilities identified during vulnerability scans to determine that controls within the environment were modified and implemented to mitigate vulnerabilities identified as part of vulnerability scan results.	No exceptions noted.
			Inspected the information security policy regarding the process for implementing security controls to mitigate vulnerabilities identified during vulnerability scans to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures identified as part of the various evaluations performed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the various assessments performed on the environment and supporting incident tickets for a sample of vulnerabilities identified from a vulnerability scan to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures identified as part of the various evaluations performed.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the 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 internal controls matrix and supporting materials and management meeting invite and emails 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 internal controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the disaster recovery and contingency plan 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 disaster recovery and contingency plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the organizational chart and the 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.

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**
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet.	Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's intranet.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	Inspected the internal controls matrix to determine that management documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the internal controls matrix to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.
		As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the completed risk assessment to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management.	No exceptions noted.
		The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Authentication of access • Protecting the entity's assets from external threats	Inspected the internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to: • Restricting access rights to authorized users • Authentication of access • Protecting the entity's assets from external threats	No exceptions noted.
		Management has established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	Inspected the internal controls matrix to determine that management established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management meeting invite and emails to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.	Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.	No exceptions noted.
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's intranet.	Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's intranet.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.	Inspected the organizational chart and job descriptions and determined that responsible parties were defined and assigned to coordinate and monitor risk management, compliance and audit activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel.	Inspected the organizational and information security policies and procedures to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	No exceptions noted.
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and the internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	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 key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the internal controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.
		Process owners and management operate the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and the internal controls matrix to determine that process owners and management operated the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	No exceptions noted.
		The effectiveness of the internal controls implemented within the environment is evaluated annually.	Inspected the meeting invite and emails to determine that the effectiveness of the internal controls implemented within the environment was 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 system assets and components to determine that an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policy 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 CEO 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 to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Network user access is restricted via role-based security privileges defined within the access control system.	Inquired of the CEO regarding network access to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the network 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 authorized personnel.	Inquired of the CEO regarding administrative access to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
		Network users are authenticated via individually assigned user accounts and passwords.	Inspected the Microsoft Entra admin center to determine that network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		The network is configured to enforce password requirements that include: • Password history • Minimum password length	Inspected the network password settings to determine that the network was configured to enforce password requirements that included: • Password history • Minimum password length	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout observation window	Inspected the network account lockout settings to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout observation window	No exceptions noted.
		Network audit logging configurations are in place that include: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	No exceptions noted.
		Network audit logs are maintained for review when needed.	Inquired of the CEO regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained for review when needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inspected the firewall settings and the cloud environment to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.
		Data coming into the environment is secured and monitored through the use of firewalls and an IDS.	Inspected the 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.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the information security policy and the encryption configurations for data in transit to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the AES.	Inspected the information security policy and the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		Encryption keys are protected during generation, storage, use, and destruction.	Inquired of the CEO regarding the encryption keys 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**
			Inspected the encryption policies and procedures to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
		Logical access reviews are performed annually.	Inquired of the CEO regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the information security policy for the in-scope systems regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the completed access review for the in-scope systems to determine that logical access reviews were performed annually.	Testing of the control activities disclosed that logical access reviews were not performed within the review period. Subsequent testing disclosed that logical access reviews were performed after the review period.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the CEO regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the onboarding procedures, the in-scope user listings, and the user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the CEO regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the hiring and termination policies and procedures regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the employee offboarding procedures, the in-scope user listings, and the user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked 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**
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policy to determine 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 CEO 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 to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews are performed annually.	Inquired of the CEO regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the information security policy for the in-scope systems regarding user access reviews to determine that logical access reviews were performed 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**
			Inspected the completed access review for the in-scope systems to determine that logical access reviews were performed annually.	Testing of the control activities disclosed that logical access reviews were not performed within the review period. Subsequent testing disclosed that logical access reviews were performed after the review period.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the CEO regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the onboarding procedures, the in-scope user listings, and the user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the CEO regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the hiring and termination policies and procedures regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the employee offboarding procedures, the in-scope user listings, and the user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process.	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.	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 the 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.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policy 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 CEO regarding privileged access 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 to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews are performed annually.	Inquired of the CEO regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the information security policy for the in-scope systems regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the completed access review for the in-scope systems to determine that logical access reviews were performed annually.	Testing of the control activities disclosed that logical access reviews were not performed within the review period. Subsequent testing disclosed that logical access reviews were performed after the review period.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the CEO regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the onboarding procedures, the in-scope user listings, and the user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the CEO regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the hiring and termination policies and procedures regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the employee offboarding procedures, the in-scope user listings, and the user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process.	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	Logical access to systems is revoked as a component of the termination process.	Inquired of the CEO regarding the offboarding process to determine that logical access to systems was revoked 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**
	to meet the entity's objectives.		Inspected the hiring and termination policies and procedures regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the employee offboarding procedures, the in-scope user listings, and the user access revocation ticket for an example terminated employee to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
		Policies and procedures are in place to guide personnel in physical security activities.	Inspected the building security policy to determine that policies and procedures were in place to guide personnel in physical security activities.	No exceptions noted.
		Physical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the onboarding procedures, the badge access listings and the user access request ticket for an example new hire to determine that physical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		A manned reception desk is in place to monitor and control access to the entrance of the office facility during standard business hours.	Inquired of the CEO regarding facility access controls to determine that a manned reception desk was in place to monitor and control access to the entrance of the office facility during standard business hours.	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
			Observed the reception area in the facility to determine that a manned reception desk was in place to monitor and control access to the entrance of the office facility during standard business hours.	No exceptions noted.
			Inspected the reception area in the facility to determine that a manned reception desk was in place to monitor and control access to the entrance of the office facility during standard business hours.	No exceptions noted.
		A badge access system controls access to and within the office facility.	Inquired of the CEO regarding facility access controls to determine that a badge access system controlled access to and within the facility.	No exceptions noted.
			Observed the presence of badge access points within the facility to determine that a badge access system controlled access to and within the facility.	No exceptions noted.
			Inspected the badge access listing and zone definitions to determine that a badge access system controlled access to and within the facility.	No exceptions noted.
		Personnel are assigned to predefined badge access security zones based on job responsibilities.	Inspected the badge access listing and zone definitions to determine that personnel were assigned to predefined badge access security zones based on job responsibilities.	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 badge access system logs successful and failed physical access attempts. The logs can be pulled for review if necessary.	Inspected an example badge access log to determine that the badge access system logged successful and failed physical access attempts, and that the logs could be pulled for review if necessary.	No exceptions noted.
		Privileged access to the badge access system is restricted to authorized personnel.	Inquired of the CEO regarding privileged access to determine that privileged access to the badge access system was restricted to authorized personnel.	No exceptions noted.
			Inspected the badge access system administrator listing to determine that privileged access to the badge access system was restricted to authorized personnel.	No exceptions noted.
		Access to the data center is restricted to authorized personnel.	Inquired of the CEO regarding access the data center to determine that access to the data center was restricted to authorized personnel.	No exceptions noted.
			Inspected the data center access listing to determine that access to the data center was restricted to authorized personnel.	No exceptions noted.
		A video surveillance system is in place with footage retained for as long as the hard drive has space.	Inquired of the CEO regarding the video surveillance system throughout the facility to determine that a video surveillance system was in place with footage retained for as long as the hard drive has space.	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**
			Observed the video surveillance system throughout the facility to determine that a video surveillance system was in place with footage retained for as long as the hard drive has space.	No exceptions noted.
			Inspected the video surveillance system configurations and the oldest retained video surveillance footage to determine that a video surveillance system was in place with footage retained for as long as the hard drive has space.	No exceptions noted.
		Visitors to the office facility and data center are required to be escorted by an authorized employee.	Inquired of the CEO regarding the visitor process to determine that visitors to the office facility and data center were required to be escorted by an authorized employee.	No exceptions noted.
			Observed the overall visitor process to determine that visitors to the office facility and data center were required to be escorted by an authorized employee.	No exceptions noted.
			Inspected the physical security policies and procedures to determine that visitors to the office facility and data center were required to be escorted by an authorized employee.	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**
		Visitors to the office facility and data center are required to sign a visitor log upon arrival.	Inspected an example visitor log to determine that visitors to the facility and data center were required to sign a visitor log upon arrival.	No exceptions noted.
		Physical access is reviewed on an annual basis.	Inquired of the CEO regarding the process for reviewing physical access to determine that physical access was reviewed on an annual basis.	No exceptions noted.
			Inspected the physical access review to determine that physical access was reviewed on an annual basis.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.	Inspected the data disposal and destruction policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		Data that is no longer required is disposed of and rendered unreadable to meet the entity's objectives.	Inspected the data disposal and destruction policies and procedures and the supporting service ticket for an example request to dispose of data to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the information security policy and the encryption configurations for data in transit to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the AES.	Inspected the information security policy and the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that TLS 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and the centralized firewall rule sets 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 and the centralized firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS and IPS are utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS and IPS configurations to determine that an IDS and IPS were utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS and IPS are configured to notify personnel upon intrusion detection and prevention.	Inspected the IDS and IPS configurations, and an example alert notification to determine that the IDS and IPS were configured to notify personnel upon intrusion detection and prevention.	No exceptions noted.
		Centralized antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software.	Inspected the centralized antivirus software configurations to determine that centralized antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the centralized 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 centralized antivirus software provider pushes updates to the installed centralized antivirus software as new updates are available.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software provider pushed updates to the installed centralized antivirus software as new updates were available.	No exceptions noted.
		The centralized antivirus software is configured to scan workstations in real-time.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software was configured to scan workstations in real-time.	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.	Passwords and production data is stored in an encrypted format using software supporting the AES.	Inspected the information security policy and the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.

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
		TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and the centralized firewall rule sets 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 and the centralized firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS and IPS are utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS and IPS configurations to determine that an IDS and IPS were utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS and IPS are configured to notify personnel upon intrusion detection and prevention.	Inspected the IDS and IPS configurations, and an example alert notification to determine that the IDS and IPS were configured to notify personnel upon intrusion detection and prevention.	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**
		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.
		The ability to restore backups is restricted to authorized personnel.	Inquired of the CEO regarding restoring backed up data to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of users with the ability to restore backups to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.
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.	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 centralized antivirus software configurations, the IDS configurations, the IPS configurations, and the firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.

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**
		Centralized antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software.	Inspected the centralized antivirus software configurations to determine that centralized antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the centralized antivirus software.	No exceptions noted.
		The centralized antivirus software provider pushes updates to the installed centralized antivirus software as new updates are available.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software provider pushed updates to the installed centralized antivirus software as new updates were available.	No exceptions noted.
		The centralized antivirus software is configured to scan workstations in real-time.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software was configured to scan workstations in real-time.	No exceptions noted.
		The ability to install applications and software on workstations is restricted to authorized personnel.	Inquired of the CEO regarding the applications and software to determine that the ability to install applications and software on workstations was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of users with the ability to install applications and software on workstations 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**
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and an example alert notification, and the IDS and IPS configurations and an example alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds had been exceeded.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	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 centralized antivirus software configurations, the IDS configurations, the IPS configurations, and the firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Internal vulnerability scans are performed annually and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results report to determine that internal vulnerability scans were performed annually and remedial actions were taken where necessary.	No exceptions noted.
		A third party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the network and infrastructure security policy to determine that a third party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and the centralized firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and the centralized firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS and IPS are utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS and IPS configurations to determine that an IDS and IPS were utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS and IPS are configured to notify personnel upon intrusion detection and prevention.	Inspected the IDS and IPS configurations, and an example alert notification to determine that the IDS and IPS were configured to notify personnel upon intrusion detection and prevention.	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.
		Management defined configuration standards in the information security policies and procedures.	Inspected the information security policies and procedures to determine that management defined configuration standards in the information security policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and an example alert notification, and the IDS and IPS configurations and an example alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds had been exceeded.	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 management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
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.	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 centralized antivirus software configurations, the IDS configurations, the IPS configurations, and the firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.

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 account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout observation window	Inspected the network account lockout settings to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout observation window	No exceptions noted.
		Network audit logging configurations are in place that include: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	No exceptions noted.
		Network audit logs are maintained for review when needed.	Inquired of the CEO regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained for review when needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Operating system account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout observation window	Inspected the account lockout configurations for a sample of production servers to determine that production server account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Operating system audit logging configurations are in place that include: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	Inspected the audit logging configurations for a sample of production servers and an example production server audit log extract to determine that production server audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Operating system audit logs are maintained for review when needed.	Inquired of the CEO regarding production server audit logs to determine that production server audit logs were maintained for review when needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected an example production server audit log extract to determine that production server audit logs were maintained for review when needed.	No exceptions noted.
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the account lockout configurations for a sample of production databases to determine that operating system account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Production database audit logging configurations are in place to log user activity.	Inspected the production databases audit logging configurations and an example production database audit log extract to determine that production databases audit logging configurations were in place to log user activity.	No exceptions noted.
		Production database audit logs are maintained for review when needed.	Inquired of the CEO regarding the production databases audit logs to determine that the production databases audit logs were maintained for review when needed.	No exceptions noted.
			Inspected an example production database audit log extract to determine that production databases audit logs were maintained for review when needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Production application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the production application account lockout configurations to determine that application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		The badge access system logs successful and failed physical access attempts. The logs can be pulled for review if necessary.	Inspected an example badge access log to determine that the badge access system logged successful and failed physical access attempts, and that the logs could be pulled for review if necessary.	No exceptions noted.
		A video surveillance system is in place with footage retained for as long as the hard drive has space.	Inquired of the CEO regarding the video surveillance system throughout the facility to determine that a video surveillance system was in place with footage retained for as long as the hard drive has space.	No exceptions noted.
			Observed the video surveillance system throughout the facility to determine that a video surveillance system was in place with footage retained for as long as the hard drive has space.	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 video surveillance system configurations and the oldest retained video surveillance footage to determine that a video surveillance system was in place with footage retained for as long as the hard drive has space.	No exceptions noted.
		Visitors to the office facility and data center are required to sign a visitor log upon arrival.	Inspected an example visitor log to determine that visitors to the facility and data center were required to sign a visitor log upon arrival.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and the centralized firewall rule sets 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 and the centralized firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS and IPS are utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS and IPS configurations to determine that an IDS and IPS were utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The IDS and IPS are configured to notify personnel upon intrusion detection and prevention.	Inspected the IDS and IPS configurations, and an example alert notification to determine that the IDS and IPS were configured to notify personnel upon intrusion detection and prevention.	No exceptions noted.
		Centralized antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software.	Inspected the centralized antivirus software configurations to determine that centralized antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the centralized antivirus software.	No exceptions noted.
		The centralized antivirus software provider pushes updates to the installed centralized antivirus software as new updates are available.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software provider pushed updates to the installed centralized antivirus software as new updates were available.	No exceptions noted.
		The centralized antivirus software is configured to scan workstations in real-time.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software was configured to scan workstations in real-time.	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.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">System Operations</th></tr>
<tr><th>CC7.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>The monitoring software is configured to alert IT personnel when thresholds have been exceeded.</td><td>Inspected the monitoring tool configurations and an example alert notification, and the IDS and IPS configurations and an example alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds had been exceeded.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.</td><td>Inspected the information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>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.</td><td>Inquired of the CEO regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.</td><td>No exceptions noted.</td></tr>
</table>

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">System Operations</th></tr>
<tr><th>CC7.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td></td><td>Inspected the information security policy regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>CCTV cameras monitor physical access to the entity's office facilities and visitor access to the office facilities and server room / data center require the visitor to sign a visitor log prior upon arrival.</td><td>Inquired of the CEO regarding cameras to determine that CCTV cameras monitored physical access to the entity's office facilities and visitor access to the office facilities and server room required the visitor to sign a visitor log prior upon arrival.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Observed the CCTV cameras in place at the entity's office facilities and server room to determine that CCTV cameras monitored physical access to the entity's office facilities and visitor access to the office facilities and server room required the visitor to sign a visitor log prior upon arrival.</td><td>No exceptions noted.</td></tr>
</table>

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 visitor log for an example month to determine that CCTV cameras monitored physical access to the entity's facilities and visitor access to the facility and server room required the visitor to sign a visitor log prior upon arrival.	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 the management reports and risk management reports 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.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inquired of the CEO regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the information security policy regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inquired of the CEO regarding annual review process for incident response and escalation procedures and the documentation of such reviews, including any identified updates or improvements to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
			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.

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 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.	Inquired of the CEO regarding incident response to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the CEO regarding security incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the information security policy to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that no security incidents occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the CEO regarding the process for documenting, tracking, and updating incidents within the standardized ticketing system to reflect planned resolution to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the information security policy to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident tickets within the standardized ticketing system and incident management procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of CEO regarding security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the incident response policies and procedures regarding security incidents to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	Testing of the control activities determined that no security incidents occurred during the review period.
		Identified incidents are reviewed, monitored and investigated by an incident response team.	Inquired of CEO regarding security incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
			Inspected the information security policies to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	Testing of the control activities determined that no security incidents occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inquired of the CEO regarding critical security incidents 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 information security policies 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 ticket for a sample of 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 the control activities determined that no critical security incidents occurred during the review period.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inquired of the CEO regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the information security policy regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		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 the management reports and risk management reports 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.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inquired of the CEO regarding annual review process for incident response and escalation procedures and the documentation of such reviews, including any identified updates or improvements to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	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 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.
			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.	Inquired of the CEO regarding incident response to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the CEO regarding security incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the information security policy to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the CEO regarding the process for documenting, tracking, and updating incidents within the standardized ticketing system to reflect planned resolution to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the information security policy to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident tickets within the standardized ticketing system and incident management procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of CEO regarding security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the incident response policies and procedures regarding security incidents to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	Testing of the control activities determined that no security incidents occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the incident response policies and procedures to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented.	No exceptions noted.
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inquired of the CEO regarding security incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
			Inspected the information security policies for a sample of incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	Testing of the control activities determined that no security incidents occurred during the review period.
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the information security policy to determine that documented incident response and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Critical security incidents that result in a service/business operation disruption are communicated to those affected through creation of an incident ticket.	Inquired of the CEO regarding critical security incidents to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through creation of an incident ticket.	No exceptions noted.
			Inspected the information security policies regarding critical security incidents to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through creation of an incident ticket.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security 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 creation of an incident ticket.	Testing of the control activities determined that no critical security incidents occurred during the review period.
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.	Inquired of the CEO regarding 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.

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 information security policies regarding 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.
			Inspected the supporting incident ticket for a sample of incidents to determine that the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	Testing of the control activities determined that no critical security incidents occurred during the review period.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	A data backup restoration test is performed on an annual basis.	Inquired of the CEO regarding restoration testing to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the disaster recovery and contingency plan to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the disaster recovery and contingency plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	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 the management reports and risk management reports 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.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of CEO regarding security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the incident response policies and procedures regarding security incidents 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**
			Inspected the supporting incident ticket for a sample of critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	Testing of the control activities determined that no security incidents occurred during the review period.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		A disaster recovery and contingency plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the disaster recovery and contingency plan to determine that a disaster recovery and contingency 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 and contingency plan and procedures are updated based on disaster recovery and contingency plan test results.	Inspected the disaster recovery and contingency plan and completed disaster recovery and contingency plan test results to determine that the disaster recovery and contingency plan and procedures were updated based on disaster recovery and contingency plan test results.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Authorization of change requests - Owner or business unit manager • Development - Application Design and Support Department • Testing - Quality Assurance Department • Implementation - Software Change Management Group	Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests - Owner or business unit manager • Development - Application Design and Support Department • Testing - Quality Assurance Department • Implementation - Software Change Management Group	No exceptions noted.
		System changes are communicated to both affected internal and external users.	Inspected the change emails to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inquired of the CEO regarding infrastructure changes to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the change management policies and procedures to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.
			Inspected the supporting change ticket for a sample of infrastructure and operating system to determine that system changes were authorized and approved by management prior to implementation.	Testing of the control activities disclosed that no infrastructure changes occurred during the review period.
		System patches/security updates follow the standard change management process.	Inspected the patch management policies and procedures to determine that system patches/security updates follow the standard patch management process.	No exceptions noted.
		System patches/security updates are performed on a configured schedule.	Inquired of the CEO regarding the schedule for applying system patches and security updates to determine that system patches security updates were performed on a configured schedule.	No exceptions noted.
			Inspected the system patching configurations and an example patching job to determine that system patches/security updates were performed on a configured schedule.	No exceptions noted.

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.	Inquired of the CEO regarding infrastructure changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
			Inspected the change management policies and procedures to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
			Inspected the supporting change ticket for a sample of infrastructure and operating system to determine that system change requests were documented and tracked in a ticketing system.	Testing of the control activities disclosed that no infrastructure changes occurred during the review period.
		Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.	Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the security management process policy to determine that management had defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk assessment and management policies and procedures and completed risk assessment 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 one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the documented security management process and the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the documented security management process and the completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		Documented policies and procedures are in place to guide personnel in performing risk assessment and risk mitigation activities.	Inspected the risk assessment and management policies and procedures to determine that documented policies and procedures were in place to guide personnel in performing risk assessment and risk mitigation activities.	No exceptions noted.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.

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.	Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment 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.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the security management process policy to determine that management had defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third parties to evaluate the effectiveness of controls within the vendor or third party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third parties to evaluate the effectiveness of controls within the vendor or third party's environment.	No exceptions noted.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.	Inspected the vendor risk assessment policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.	No exceptions noted.
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment to determine that management developed third-party risk mitigation strategies to address risks identified during the third-party risk assessment process.	No exceptions noted.
		Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Risk Mitigation

CC9.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The entity's third-party 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	Inquired of the CEO the third-party agreement to determine that the third-party agreement outlines and communicates the scope of services, roles and responsibilities, terms of the business relationship, communication protocols, compliance requirements, service levels, and just cause for terminating the relationship.	No exceptions noted.
			Inspected the vendor management policies and procedures to determine that the entity's third-party agreement outlined and communicated: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Risk Mitigation</th></tr>
<tr><th>CC9.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td></td><td>Inspected the master third-party agreement template and third-party agreement for a sample of third parties to determine that the entity's third-party agreement outlined and communicated:
• The scope of services
• Roles and responsibilities
• Terms of the business relationship
• Communication protocols
• Compliance requirements
• Service levels
• Just cause for terminating the relationship</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements.</td><td>Inspected the vendor risk assessment policies and procedures to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Management has assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.</td><td>Inspected the organizational chart and job descriptions to determine that management assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management has established exception handling procedures for services provided by third parties.	Inspected the third-party and vendor policies and procedures 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 third-party and vendor policies and procedures 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 third-party and vendor policies and procedures 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.	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 centralized antivirus software configurations, the IDS configurations, the IPS configurations, and the firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Internal vulnerability scans are performed annually and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results report to determine that internal vulnerability scans were performed annually and remedial actions were taken where necessary.	No exceptions noted.
		A third party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the network and infrastructure security policy to determine that a third party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout observation window	Inspected the network account lockout settings to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout observation window	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network audit logging configurations are in place that include: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	No exceptions noted.
		Network audit logs are maintained for review when needed.	Inquired of the CEO regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained for review when needed.	No exceptions noted.
		An IDS and IPS are utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS and IPS configurations to determine that an IDS and IPS were utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS and IPS are configured to notify personnel upon intrusion detection and prevention.	Inspected the IDS and IPS configurations, and an example alert notification to determine that the IDS and IPS were configured to notify personnel upon intrusion detection and prevention.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Centralized antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software.	Inspected the centralized antivirus software configurations to determine that centralized antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the centralized antivirus software.	No exceptions noted.
		The centralized antivirus software provider pushes updates to the installed centralized antivirus software as new updates are available.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software provider pushed updates to the installed centralized antivirus software as new updates were available.	No exceptions noted.
		The centralized antivirus software is configured to scan workstations in real-time.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software was configured to scan workstations in real-time.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations and an example alert notification, and the IDS and IPS configurations and an example alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds had been exceeded.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inquired of the CEO regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
			Inspected the information security policy regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Policies and procedures are in place regarding preventing, detecting, containing, and correcting security violations.	Inspected the information security policy to determine that policies and procedures were in place regarding preventing, detecting, containing, and correcting security violations.	No exceptions noted.

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

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

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

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the documented security management process and the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the documented security management process and the completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		Internal vulnerability scans are performed annually and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results report to determine that internal vulnerability scans were performed annually and remedial actions were taken where necessary.	No exceptions noted.
		A third party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the network and infrastructure security policy to determine that a third party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram and the centralized firewall rule sets 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 and the centralized firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS and IPS are utilized to analyze network events and report possible or actual network security breaches.	Inspected the IDS and IPS configurations to determine that an IDS and IPS were utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS and IPS are configured to notify personnel upon intrusion detection and prevention.	Inspected the IDS and IPS configurations, and an example alert notification to determine that the IDS and IPS were configured to notify personnel upon intrusion detection and prevention.	No exceptions noted.
		Centralized antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software.	Inspected the centralized antivirus software configurations to determine that centralized antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the centralized antivirus software.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The centralized antivirus software provider pushes updates to the installed centralized antivirus software as new updates are available.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software provider pushed updates to the installed centralized antivirus software as new updates were available.	No exceptions noted.
		The centralized antivirus software is configured to scan workstations in real-time.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software was configured to scan workstations in real-time.	No exceptions noted.
164.308 (a)(1)(ii)(C)	**Sanction policy:** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the company handbook to determine that sanction policies, which included probation, suspension and termination, were in place for employee misconduct.	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.	Network audit logging configurations are in place that include: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	No exceptions noted.
		Network audit logs are maintained for review when needed.	Inquired of the CEO regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected an example network audit log extract to determine that network audit logs were maintained for review when needed.	No exceptions noted.
164.308 (a)(2)	**Assigned security responsibility:** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	Responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI is formally documented and assigned to a job role.	Inspected the Chief Executive Officer (CEO) job description and the organizational chart to determine that responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI was formally documented and assigned to a job role.	No exceptions noted.
164.308 (a)(3)(i)	**Workforce security:** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under the Information Access Management standard and to prevent those who do not have appropriate access from obtaining access to ePHI. Policies and procedures should include Authorization and/or Supervision procedures, Workforce Clearance Procedure, and Termination Procedures.	Policies and procedures are formally defined and documented regarding authorization of access to ePHI.	Inspected the information security policy to determine that policies and procedures were formally defined and documented regarding authorization of access to ePHI.	No exceptions noted.
		Users accessing ePHI are authenticated via individually assigned user accounts and passwords to only authorized personnel.	Inquired of the CEO regarding user access to ePHI to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Observed a user login to the network that maintains ePHI to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the network password configurations to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Access to ePHI is restricted to authorized personnel.	Inquired of the CEO regarding access to ePHI to determine that access to ePHI was restricted to authorized personnel.	No exceptions noted.
			Inspected the network user access listings to determine that access to ePHI was restricted to authorized personnel.	No exceptions noted.
		Users with access to ePHI are reviewed by management annually.	Inspected the completed user access review to determine that users with access to ePHI were reviewed by management annually.	No exceptions noted.
164.308 (a)(3)(ii)(A)	**Authorization and/or supervision:** Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the CEO regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the onboarding procedures, the in-scope user listings, and the user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the CEO regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
		Policies and procedures are formally defined and documented regarding authorization of access to ePHI.	Inspected the information security policy to determine that policies and procedures were formally defined and documented regarding authorization of access to ePHI.	No exceptions noted.
164.308 (a)(3)(ii)(B)	**Workforce clearance procedure:** Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Policies and procedures are formally defined and documented regarding authorization of access to ePHI.	Inspected the information security policy to determine that policies and procedures were formally defined and documented regarding authorization of access to ePHI.	No exceptions noted.
		Users accessing ePHI are authenticated via individually assigned user accounts and passwords to only authorized personnel.	Inquired of the CEO regarding user access to ePHI to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Observed a user login to the network that maintains ePHI to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the network password configurations to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Access to ePHI is restricted to authorized personnel.	Inquired of the CEO regarding access to ePHI to determine that access to ePHI was restricted to authorized personnel.	No exceptions noted.
			Inspected the network user access listings to determine that access to ePHI was restricted to authorized personnel.	No exceptions noted.
		Users with access to ePHI are reviewed by management annually.	Inspected the completed user access review for an example quarter to determine that users with access to ePHI were reviewed by management annually.	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:** Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [the Workforce Clearance Procedure] of this section.	Logical access to systems is revoked as a component of the termination process.	Inquired of the CEO regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the hiring and termination policies and procedures regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the employee offboarding procedures, the in-scope user listings, and the user access revocation ticket for an example terminated employee to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
		Policies and procedures are formally defined and documented regarding revoking access following termination.	Inspected the documented employee offboarding procedures to determine that policies and procedures were formally defined and documented regarding revoking access following termination.	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)(i)	**Information access management:** Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of the Privacy Rule. Policies and procedures should include: Isolating Health Care Clearinghouse Functions, Access Authorization and Access Establishment and Modification.	Management maintains policies and procedures that ensure the authorization of access to ePHI and are consistent with the applicable requirements of the Privacy Rule.	Inspected the information security policy to determine that management maintained policies and procedures that ensured the authorization of access to ePHI and were consistent with the applicable requirements of the Privacy Rule.	No exceptions noted.
164.308 (a)(4)(ii)(A)	**Isolating healthcare clearinghouse functions:** If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Not Applicable. The entity is not a healthcare clearinghouse.	Not Applicable.	Not Applicable.
164.308 (a)(4)(ii)(B)	**Access authorization:** Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.	Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the CEO regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the onboarding procedures, the in-scope user listings, and the user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the CEO regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
		Policies and procedures are formally defined and documented regarding authorization of access to ePHI.	Inspected the information security policy to determine that policies and procedures were formally defined and documented regarding authorization of access to ePHI.	No exceptions noted.
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.	Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the CEO regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the onboarding procedures, the in-scope user listings, and the user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.

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.	Inquired of the CEO regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the hiring and termination policies and procedures regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the employee offboarding procedures, the in-scope user listings, and the user access revocation ticket for an example terminated employee to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
		Policies and procedures are formally defined and documented regarding authorization of access to ePHI.	Inspected the information security policy to determine that policies and procedures were formally defined and documented regarding authorization of access to ePHI.	No exceptions noted.
		Users with access to ePHI are reviewed by management annually.	Inspected the completed user access review for an example quarter to determine that users with access to ePHI were reviewed by management annually.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.308 (a)(5)(i)	**Security awareness and training:** Implement a security awareness and training program for all members of the workforce (including management).	Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the security and awareness training policy to determine that employees were required to attend continued training annually that related to their job role and responsibilities.	No exceptions noted.
	Component of the Security Awareness and Training program should include Security Reminders, Protection Malicious Software, Log-in Monitoring and Password Management.	Executive management has created a training program for its employees.	Inspected the information security and awareness training program to determine that executive management had created a training program for its employees.	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.	Inquired of the CEO regarding periodic security reminders to determine that users were made aware of security updates and updates to security policies.	No exceptions noted.
			Inspected the security shorts report to determine that users were made aware of security updates and updates to security policies.	No exceptions noted.
164.308 (a)(5)(ii)(B)	**Protection from malicious software:** Procedures for guarding against, detecting, and reporting malicious software.	Centralized antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software.	Inspected the centralized antivirus software configurations to determine that centralized antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the centralized antivirus software.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The centralized antivirus software provider pushes updates to the installed centralized antivirus software as new updates are available.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software provider pushed updates to the installed centralized antivirus software as new updates were available.	No exceptions noted.
		The centralized antivirus software is configured to scan workstations in real-time.	Inspected the centralized antivirus software configurations to determine that the centralized antivirus software was configured to scan workstations in real-time.	No exceptions noted.
		Policies and procedures are formally documented regarding preventing, detecting, and reporting the presence of malicious software.	Inspected the information security policy to determine that policies and procedures were formally documented regarding preventing, detecting, and reporting the presence of malicious software.	No exceptions noted.
164.308 (a)(5)(ii)(C)	**Log-in monitoring:** Procedures for monitoring log-in attempts and reporting discrepancies.	Network audit logging configurations are in place that include: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	No exceptions noted.
		Network audit logs are maintained for review when needed.	Inquired of the CEO regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected an example network audit log extract to determine that network audit logs were maintained for review when needed.	No exceptions noted.
164.308 (a)(5)(ii)(D)	**Password management:** Procedures for creating, changing, and safeguarding passwords.	The network is configured to enforce password requirements that include: • Password history • Minimum password length	Inspected the network password settings to determine that the network was configured to enforce password requirements that included: • Password history • Minimum password length	No exceptions noted.
		Policies are in place to guide personnel in creating, changing, and safeguarding passwords.	Inspected the information security policy to determine that policies were in place to guide personnel in creating, changing, and safeguarding passwords.	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.	Inquired of the CEO regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the information security policy regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inquired of the CEO regarding incident response to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the CEO regarding security incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the information security policy 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**
			Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the CEO regarding the process for documenting, tracking, and updating incidents within the standardized ticketing system to reflect planned resolution to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the information security policy to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident tickets within the standardized ticketing system and incident management procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that no security incidents occurred during the review period.

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 are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the information security policy 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.	Inquired of the CEO regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
			Inspected the information security policy regarding the existence, accessibility, and content of incident response and escalation procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inquired of the CEO regarding incident response to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the CEO regarding security incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the information security policy to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the CEO regarding the process for documenting, tracking, and updating incidents within the standardized ticketing system to reflect planned resolution to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the information security policy to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident tickets within the standardized ticketing system and incident management procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that no security incidents occurred during the review period.
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the information security policy 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.
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 disaster recovery and contingency plan 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 disaster recovery and contingency plan test results to determine that 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 disaster recovery and contingency plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the disaster recovery and contingency plan to determine that a disaster recovery and contingency 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 and contingency plan and procedures are updated based on disaster recovery and contingency plan test results.	Inspected the disaster recovery and contingency plan and completed disaster recovery and contingency plan test results to determine that the disaster recovery and contingency plan and procedures were updated based on disaster recovery and contingency plan test results.	No exceptions noted.
		The disaster recovery and contingency 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 disaster recovery and contingency plan test results to determine that the disaster recovery and contingency 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
164.308 (a)(7)(ii)(A)	**Data backup plan:** Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		Full backups of critical data are performed on a daily basis.	Inspected the backup schedule and configurations and an example backup log to determine that full backups of critical data were performed on a daily basis.	No exceptions noted.
		When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure.	Inquired of the CEO regarding the backup job fails 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.
			Inspected the backup policy regarding the backup job fails 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.
			Inspected the backup configurations and the backup alert for a sample of failed backups to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure.	Testing of the control activity disclosed that there were no failed backups 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)(7)(ii)(B)	**Disaster recovery plan:** Establish (and implement as needed) procedures to restore any loss of data.	A data backup restoration test is performed on an annual basis.	Inquired of the CEO regarding restoration testing to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the disaster recovery and contingency plan 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 disaster recovery and contingency plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		A disaster recovery and contingency plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the disaster recovery and contingency plan to determine that a disaster recovery and contingency 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.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The disaster recovery and contingency plan and procedures are updated based on disaster recovery and contingency plan test results.	Inspected the disaster recovery and contingency plan and completed disaster recovery and contingency plan test results to determine that the disaster recovery and contingency plan and procedures were updated based on disaster recovery and contingency plan test results.	No exceptions noted.
		The disaster recovery and contingency 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 disaster recovery and contingency plan test results to determine that the disaster recovery and contingency 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**
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 disaster recovery and contingency plan 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 disaster recovery and contingency plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		A disaster recovery and contingency plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the disaster recovery and contingency plan to determine that a disaster recovery and contingency 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 and contingency plan and procedures are updated based on disaster recovery and contingency plan test results.	Inspected the disaster recovery and contingency plan and completed disaster recovery and contingency plan test results to determine that the disaster recovery and contingency plan and procedures were updated based on disaster recovery and contingency plan test results.	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 and contingency 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 disaster recovery and contingency plan test results to determine that the disaster recovery and contingency 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)(D)	**Testing and revision procedures:** Implement procedures for periodic testing and revision of contingency plans.	A data backup restoration test is performed on an annual basis.	Inquired of the CEO regarding restoration testing to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the disaster recovery and contingency plan to determine that business continuity and disaster recovery plans were developed and updated 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**
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the disaster recovery and contingency plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		A disaster recovery and contingency plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the disaster recovery and contingency plan to determine that a disaster recovery and contingency 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 and contingency plan and procedures are updated based on disaster recovery and contingency plan test results.	Inspected the disaster recovery and contingency plan and completed disaster recovery and contingency plan test results to determine that the disaster recovery and contingency plan and procedures were updated based on disaster recovery and contingency plan test results.	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 and contingency 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 disaster recovery and contingency plan test results to determine that the disaster recovery and contingency 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.	Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the security management process policy to determine that management had defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks for each identified vulnerability	Inspected the security management process policy and the completed risk assessment to determine that the entity's risk assessment process included: • Identifying the relevant information assets that were critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks 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.	The entity maintains a policy to assess the relative criticality of applications, systems and other assets maintaining ePHI, so that such data can be properly protected during emergencies and during normal business operations.	Inspected the information security policy to determine that the entity maintained a policy to assess the relative criticality of applications, systems and other assets maintaining ePHI, so that such data can be properly protected during emergencies and during normal business operations.	No exceptions noted.
		The entity maintains an asset inventory that categorizes and prioritizes systems and other assets maintaining ePHI.	Inspected the master asset inventory to determine that the entity maintained an asset inventory that categorized and prioritized systems and other assets maintaining ePHI.	No exceptions noted.
		Internal vulnerability scans are performed annually and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results report to determine that internal vulnerability scans were performed annually and remedial actions were taken where necessary.	No exceptions noted.
		A third party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	Inspected the network and infrastructure security policy to determine that a third party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the disaster recovery and contingency plan to determine that business continuity and disaster recovery plans were developed and updated 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
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the disaster recovery and contingency plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		A disaster recovery and contingency plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the disaster recovery and contingency plan to determine that a disaster recovery and contingency 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 and contingency plan and procedures are updated based on disaster recovery and contingency plan test results.	Inspected the disaster recovery and contingency plan and completed disaster recovery and contingency plan test results to determine that the disaster recovery and contingency plan and procedures were updated based on disaster recovery and contingency plan test results.	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 and contingency 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 disaster recovery and contingency plan test results to determine that the disaster recovery and contingency 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 (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.	The entity maintained procedures to guide management in engaging in business associate agreements with businesses and subcontractors that create, receive maintain, or transmit ePHI.	Inquired of the CEO regarding business associate agreements to determine that the entity maintained business associate agreements with businesses and subcontractors that create, receive maintain, or transmit ePHI.	No exceptions noted.
			Inspected the business associates agreement template to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses and subcontractors that create, receive maintain, or transmit ePHI.	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)(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.	The entity maintained procedures to guide management in engaging in business associate agreements with businesses and subcontractors that create, receive maintain, or transmit ePHI.	Inspected the business associates agreement for a sample of new business associates to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses and subcontractors that create, receive maintain, or transmit ePHI.	Testing of the control activity disclosed that no business associates were onboard during the review period.
			Inquired of the CEO regarding business associate agreements to determine that the entity maintained business associate agreements with businesses and subcontractors that create, receive maintain, or transmit ePHI.	No exceptions noted.
			Inspected the business associates agreement template to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses and subcontractors that create, receive maintain, or transmit ePHI.	No exceptions noted.

ADMINISTRATIVE SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the business associates agreement for a sample of new business associates to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses and subcontractors that create, receive maintain, or transmit ePHI.	Testing of the control activity disclosed that no business associates were onboard during the review period.
164.308 (b)(3)	**Written contract or other arrangement:** Document the satisfactory assurances required by paragraph (b)(1) or (b2) above of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a) [the Organizational Requirements].	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: ● The boundaries of the system ● System commitments and requirements ● Terms, conditions and responsibilities between the involved parties	Inquired of the CEO regarding business associate agreements to determine that the entity maintained business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: ● The boundaries of the system ● System commitments and requirements ● Terms, conditions and responsibilities between the involved parties	No exceptions noted.

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

ADMINISTRATIVE SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the business associates agreement for a sample of new business associates to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: ● The boundaries of the system ● System commitments and requirements ● Terms, conditions and responsibilities between the involved	Testing of the control activity disclosed that no business associates were onboard during the review period.

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.	Logical access to systems is revoked as a component of the termination process.	Inquired of the CEO regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the hiring and termination policies and procedures regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the employee offboarding procedures, the in-scope user listings, and the user access revocation ticket for an example terminated employee to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
		Policies and procedures are in place to guide personnel in physical security activities.	Inspected the building security policy to determine that policies and procedures were in place to guide personnel in physical security activities.	No exceptions noted.
		Physical access to systems is approved and granted to an employee as a component of the hiring process.	Inspected the onboarding procedures, the badge access listings and the user access request ticket for an example new hire to determine that physical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A manned reception desk is in place to monitor and control access to the entrance of the office facility during standard business hours.	Inquired of the CEO regarding facility access controls to determine that a manned reception desk was in place to monitor and control access to the entrance of the office facility during standard business hours.	No exceptions noted.
			Observed the reception area in the facility to determine that a manned reception desk was in place to monitor and control access to the entrance of the office facility during standard business hours.	No exceptions noted.
			Inspected the reception area in the facility to determine that a manned reception desk was in place to monitor and control access to the entrance of the office facility during standard business hours.	No exceptions noted.
		A badge access system controls access to and within the office facility.	Inquired of the CEO regarding facility access controls to determine that a badge access system controlled access to and within the facility.	No exceptions noted.
			Observed the presence of badge access points within the facility to determine that a badge access system controlled access to and within the facility.	No exceptions noted.
			Inspected the badge access listing and zone definitions to determine that a badge access system controlled access to and within the facility.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are assigned to predefined badge access security zones based on job responsibilities.	Inspected the badge access listing and zone definitions to determine that personnel were assigned to predefined badge access security zones based on job responsibilities.	No exceptions noted.
		The badge access system logs successful and failed physical access attempts. The logs can be pulled for review if necessary.	Inspected an example badge access log to determine that the badge access system logged successful and failed physical access attempts, and that the logs could be pulled for review if necessary.	No exceptions noted.
		Privileged access to the badge access system is restricted to authorized personnel.	Inquired of the CEO regarding privileged access to determine that privileged access to the badge access system was restricted to authorized personnel.	No exceptions noted.
			Inspected the badge access system administrator listing to determine that privileged access to the badge access system was restricted to authorized personnel.	No exceptions noted.
		Access to the data center is restricted to authorized personnel.	Inquired of the CEO regarding access the data center to determine that access to the data center was restricted to authorized personnel.	No exceptions noted.
			Inspected the data center access listing to determine that access to the data center was restricted to authorized personnel.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		A video surveillance system is in place with footage retained for as long as the hard drive has space.	Inquired of the CEO regarding the video surveillance system throughout the facility to determine that a video surveillance system was in place with footage retained for as long as the hard drive has space.	No exceptions noted.
			Observed the video surveillance system throughout the facility to determine that a video surveillance system was in place with footage retained for as long as the hard drive has space.	No exceptions noted.
			Inspected the video surveillance system configurations and the oldest retained video surveillance footage to determine that a video surveillance system was in place with footage retained for as long as the hard drive has space.	No exceptions noted.
		Visitors to the office facility and data center are required to be escorted by an authorized employee.	Inquired of the CEO regarding the visitor process to determine that visitors to the office facility and data center were required to be escorted by an authorized employee.	No exceptions noted.
			Observed the overall visitor process to determine that visitors to the office facility and data center were required to be escorted by an authorized employee.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the physical security policies and procedures to determine that visitors to the office facility and data center were required to be escorted by an authorized employee.	No exceptions noted.
		Visitors to the office facility and data center are required to sign a visitor log upon arrival.	Inspected an example visitor log to determine that visitors to the facility and data center were required to sign a visitor log upon arrival.	No exceptions noted.
		Physical access is reviewed on an annual basis.	Inquired of the CEO regarding the process for reviewing physical access to determine that physical access was reviewed on an annual basis.	No exceptions noted.
			Inspected the physical access review for an example quarter to determine that physical access was reviewed on an annual basis.	No exceptions noted.
164.310 (a)(2)(i)	**Contingency operations:** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	A data backup restoration test is performed on an annual basis.	Inquired of the CEO regarding restoration testing to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the disaster recovery and contingency plan 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 disaster recovery and contingency plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		A disaster recovery and contingency plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the disaster recovery and contingency plan to determine that a disaster recovery and contingency 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 and contingency plan and procedures are updated based on disaster recovery and contingency plan test results.	Inspected the disaster recovery and contingency plan and completed disaster recovery and contingency plan test results to determine that the disaster recovery and contingency plan and procedures were updated based on disaster recovery and contingency plan test results.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The disaster recovery and contingency 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 disaster recovery and contingency plan test results to determine that the disaster recovery and contingency 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.	Policies and procedures are in place to guide personnel in physical security activities.	Inspected the building security policy to determine that policies and procedures were in place to guide personnel in physical security activities.	No exceptions noted.
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.	A badge access system controls access to and within the office facility.	Inquired of the CEO regarding facility access controls to determine that a badge access system controlled access to and within the facility.	No exceptions noted.
			Observed the presence of badge access points within the facility to determine that a badge access system controlled access to and within the facility.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the badge access listing and zone definitions to determine that a badge access system controlled access to and within the facility.	No exceptions noted.
		Personnel are assigned to predefined badge access security zones based on job responsibilities.	Inspected the badge access listing and zone definitions to determine that personnel were assigned to predefined badge access security zones based on job responsibilities.	No exceptions noted.
		The badge access system logs successful and failed physical access attempts. The logs can be pulled for review if necessary.	Inspected an example badge access log to determine that the badge access system logged successful and failed physical access attempts, and that the logs could be pulled for review if necessary.	No exceptions noted.
		Visitors to the office facility and data center are required to be escorted by an authorized employee.	Inquired of the CEO regarding the visitor process to determine that visitors to the office facility and data center were required to be escorted by an authorized employee.	No exceptions noted.
			Observed the overall visitor process to determine that visitors to the office facility and data center were required to be escorted by an authorized employee.	No exceptions noted.
			Inspected the physical security policies and procedures to determine that visitors to the office facility and data center were required to be escorted by an authorized employee.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Visitors to the office facility and data center are required to sign a visitor log upon arrival.	Inspected an example visitor log to determine that visitors to the facility and data center were required to sign a visitor log upon arrival.	No exceptions noted.
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).	Policies and procedures are formally defined and documented regarding documenting repairs and inspection reports for physical components.	Inspected the building security policy to determine that policies and procedures were formally defined and documented regarding documenting repairs and inspection reports for physical components.	No exceptions noted.
		Facility security maintenance records are created to document repairs and changes to physical elements of a facility related to security.	Inspected an example physical maintenance record to determine that facility security maintenance records were created to document repairs and changes to physical elements of a facility related to security.	No exceptions noted.
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 CEO regarding physical security controls to determine that procedures that specified the proper functions, processes, and appropriate environments of workstations that access ePHI were in place.	No exceptions noted.
			Observed the workstation areas within the facility to determine that procedures that specified the proper functions, processes, and appropriate environments of workstations that access ePHI were in place.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the building security policy 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)(1)	**Device and media control:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	Procedures are in place to ensure that maintenance records of the movements of hardware and electronic media are documented.	Inspected the transportation of external media and hardware policy and an example maintenance record for the movement of hardware and electronic media to determine that procedures were in place to ensure that maintenance records of the movements of hardware and electronic media were documented.	No exceptions noted.
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 that 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**
		Data that is no longer required is disposed of and rendered unreadable to meet the entity's objectives.	Inspected the data disposal and destruction policies and procedures and the supporting service ticket for an example request to dispose of data to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	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.	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 that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		Data that is no longer required is disposed of and rendered unreadable to meet the entity's objectives.	Inspected the data disposal and destruction policies and procedures and the supporting service ticket for an example request to dispose of data to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	No exceptions noted.
		The entity sanitizes media containing ePHI when the media is to be reused.	Inspected the information security policy to determine that the entity sanitized media containing ePHI when the media was to be reused.	No exceptions noted.

PHYSICAL SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
164.310 (d)(2)(iii)	**Accountability:** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Procedures are in place to ensure that maintenance records of the movements of hardware and electronic media are documented.	Inspected the transportation of external media and hardware policy and an example maintenance record for the movement of hardware and electronic media to determine that procedures were in place to ensure that maintenance records of the movements of hardware and electronic media were documented.	No exceptions noted.
164.310 (d)(2)(iv)	**Data backup and storage:** Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		Full backups of critical data are performed on a daily basis.	Inspected the backup schedule and configurations and an example backup log to determine that full backups of critical data were performed on a daily basis.	No exceptions noted.
		When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure.	Inquired of the CEO regarding the backup job fails 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.
			Inspected the backup policy regarding the backup job fails 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.

PHYSICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the backup configurations and the backup alert for a sample of failed backups to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure.	Testing of the control activity disclosed that there were no failed backups during the review period.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.312 (a)(1)	**Access control:** Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4) [Information Access Management].	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		The network is configured to enforce password requirements that include: • Password history • Minimum password length	Inspected the network password settings to determine that the network was configured to enforce password requirements that included: • Password history • Minimum password length	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the CEO regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the onboarding procedures, the in-scope user listings, and the user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked as a component of the termination process.	Inquired of the CEO regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the hiring and termination policies and procedures regarding the offboarding process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the employee offboarding procedures, the in-scope user listings, and the user access revocation ticket for an example terminated employee to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the CEO regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
		Users accessing ePHI are authenticated via individually assigned user accounts and passwords to only authorized personnel.	Inquired of the CEO regarding user access to ePHI to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Observed a user login to the network that maintains ePHI to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the network password configurations to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Access to ePHI is restricted to authorized personnel.	Inquired of the CEO regarding access to ePHI to determine that access to ePHI was restricted to authorized personnel.	No exceptions noted.
			Inspected the network user access listings to determine that access to ePHI was restricted to authorized personnel.	No exceptions noted.
		Users with access to ePHI are reviewed by management annually.	Inspected the completed user access review for an example quarter to determine that users with access to ePHI were reviewed by management annually.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.312 (a)(2)(i)	**Unique user identification:** Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user. Ensure that the necessary data is available in the system logs to support audit and other related business functions.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		The network is configured to enforce password requirements that include: • Password history • Minimum password length	Inspected the network password settings to determine that the network was configured to enforce password requirements that included: • Password history • Minimum password length	No exceptions noted.
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout observation window	Inspected the network account lockout settings to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout observation window	No exceptions noted.
		Network audit logging configurations are in place that include: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network audit logs are maintained for review when needed.	Inquired of the CEO regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained for review when needed.	No exceptions noted.
		Users accessing ePHI are authenticated via individually assigned user accounts and passwords to only authorized personnel.	Inquired of the CEO regarding user access to ePHI to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Observed a user login to the network that maintains ePHI to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the network password configurations to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
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 disaster recovery and contingency plan to determine that business continuity and disaster recovery plans were developed and updated on 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**
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the disaster recovery and contingency plan test results to determine that business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		A disaster recovery and contingency plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the disaster recovery and contingency plan to determine that a disaster recovery and contingency 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 and contingency plan and procedures are updated based on disaster recovery and contingency plan test results.	Inspected the disaster recovery and contingency plan and completed disaster recovery and contingency plan test results to determine that the disaster recovery and contingency plan and procedures were updated based on disaster recovery and contingency plan test results.	No exceptions noted.
		Full backups of critical data are performed on a daily basis.	Inspected the backup schedule and configurations and an example backup log to determine that full backups of critical data were performed on a daily basis.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure.	Inquired of the CEO regarding the backup job fails 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.
			Inspected the backup policy regarding the backup job fails 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.
			Inspected the backup configurations and the backup alert for a sample of failed backups to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure.	Testing of the control activity disclosed that there were no failed backups during the review period.

TECHNICAL SAFEGUARDS

Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The disaster recovery and contingency 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 disaster recovery and contingency plan test results to determine that the disaster recovery and contingency 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.
164.312 (a)(2)(iii)	**Automatic logoff:** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Workstations are configured to terminate inactive sessions after fifteen minutes of inactivity. Users are required to re-validate with a username and password to gain control of the workstation.	Inquired of the CEO regarding user lockout after a period of inactivity to determine that workstations were configured to terminate inactive sessions after fifteen minute of inactivity. Users were required to re-validate with a username and password to gain control of the workstation.	No exceptions noted.
			Observed a user inactive on their workstation for fifteen minutes to determine that workstations were configured to terminate inactive sessions after fifteen minute of inactivity. Users were required to re-validate with a username and password to gain control of the workstation.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the information security policy to determine that workstations were configured to terminate inactive sessions after fifteen minutes of inactivity, and that users were required to re-validate with a username and password to gain control of the workstation.	No exceptions noted.
164.312 (a)(2)(iv)	**Encryption and decryption:** Implement a mechanism to encrypt and decrypt ePHI.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the information security policy and the encryption configurations for data in transit to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the AES.	Inspected the information security policy and the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.

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

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network audit logging configurations are in place that include: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon and logoff events • Directory Service Access • Logon and logoff events • Special logon events	No exceptions noted.
		Network audit logs are maintained for review when needed.	Inquired of the CEO regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained for review when needed.	No exceptions noted.
164.312 (c)(1)	**Integrity:** Implement policies and procedures to protect ePHI from improper alteration or destruction.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the information security policy and the encryption configurations for data in transit to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the AES.	Inspected the information security policy and the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the CEO regarding VPN user authentication to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Mobile devices are protected through the use of secured, encrypted connections.	Inspected the information security policy to determine that mobile devices were protected through the use of secured, encrypted connections.	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.	Policies and procedures are formally documented regarding protecting ePHI from improper alteration or destruction.	Inspected the encryption policies and procedures to determine that policies and procedures were formally documented regarding protecting ePHI from improper alteration or destruction.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the information security policy and the encryption configurations for data in transit to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the AES.	Inspected the information security policy and the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the CEO regarding VPN user authentication to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Observed the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Mobile devices are protected through the use of secured, encrypted connections.	Inspected the information security policy to determine that mobile devices were protected through the use of secured, encrypted connections.	No exceptions noted.
		Policies and procedures are formally documented regarding protecting ePHI from improper alteration or destruction.	Inspected the encryption policies and procedures to determine that policies and procedures were formally documented regarding protecting ePHI from improper alteration or destruction.	No exceptions noted.
164.312 (d)	**Person or entity authentication:** Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policy to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The network is configured to enforce password requirements that include: • Password history • Minimum password length	Inspected the network password settings to determine that the network was configured to enforce password requirements that included: • Password history • Minimum password length	No exceptions noted.
		Users accessing ePHI are authenticated via individually assigned user accounts and passwords to only authorized personnel.	Inquired of the CEO regarding user access to ePHI to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Observed a user login to the network that maintains ePHI to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
			Inspected the network password configurations to determine that users accessing ePHI were authenticated via individually assigned user accounts and passwords.	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 TLS encryption with a trusted certificate authority.	Inspected the information security policy and the encryption configurations for data in transit to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the CEO regarding VPN user authentication to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Mobile devices are protected through the use of secured, encrypted connections.	Inspected the information security policy to determine that mobile devices were protected through the use of secured, encrypted connections.	No exceptions noted.

TECHNICAL SAFEGUARDS

Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
164.312 (e)(2)(i)	**Integrity controls:** Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	Policies and procedures are formally documented regarding protecting ePHI from improper alteration or destruction.	Inspected the encryption policies and procedures to determine that policies and procedures were formally documented regarding protecting ePHI from improper alteration or destruction.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the information security policy and the encryption configurations for data in transit to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the CEO regarding VPN user authentication to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.

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.		Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Mobile devices are protected through the use of secured, encrypted connections.	Inspected the information security policy to determine that mobile devices were protected through the use of secured, encrypted connections.	No exceptions noted.
		Policies and procedures are formally documented regarding protecting ePHI from improper alteration or destruction.	Inspected the encryption policies and procedures to determine that policies and procedures were formally documented regarding protecting ePHI from improper alteration or destruction.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the information security policy and the encryption configurations for data in transit to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the AES.	Inspected the information security policy and the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations and the VPN authentication configurations to determine that TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inquired of the CEO regarding VPN user authentication to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Observed the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Mobile devices are protected through the use of secured, encrypted connections.	Inspected the information security policy to determine that mobile devices were protected through the use of secured, encrypted connections.	No exceptions noted.

TECHNICAL SAFEGUARDS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Policies and procedures are formally documented regarding the mechanisms used to encrypt ePHI.	Inspected the encryption policies and procedures to determine that policies and procedures were formally documented regarding the mechanisms used to encrypt ePHI.	No exceptions noted.

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

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

ORGANIZATIONAL REQUIREMENTS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the business associates agreement template to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved	No exceptions noted.
			Inspected the business associates agreement for a sample of new business associates to determine that the entity maintained procedures to guide management in engaging in business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicated: • The boundaries of the system • System commitments and requirements • Terms, conditions and responsibilities between the involved	Testing of the control activity disclosed that no business associates were onboard during the review period.

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

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

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

ORGANIZATIONAL REQUIREMENTS				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Policies and procedures are created and maintained in written and electronic form.	Inspected the entity's policies and procedures to determine that policies and procedures were created and maintained in written and electronic form.	No exceptions noted.
		HIPAA related incidents and events are documented in a ticketing system.	Inspected the incident management ticketing tool to determine that HIPAA related incidents and events were documented in a ticketing system.	No exceptions noted.
164.316 (b)(2)(i)	**Time Limit:** Retain the documentation required by paragraph (b) (1) of this section for 6 years for the date of its creation or the date when it last was in effect, whichever is later.	Policies and procedures are appropriately retained for a minimum of six years from the date it was created or when it was last in effect, whichever is later.	Inspected the data retention and disposal policies and procedures to determine that policies and procedures were appropriately retained for a minimum of six years from the date when it was last in effect, whichever was later.	No exceptions noted.
164.316 (b)(2)(ii)	**Availability:** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	Inspected the revision history of the information security policies and the entity's intranet to determine that policies and procedures were reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	No exceptions noted.
164.316 (b)(2)(iii)	**Updates:** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	Inspected the revision history of the information security policies and the entity's intranet to determine that policies and procedures were reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.	No exceptions noted.

BREACH NOTIFICATION				
Ref	Regulation	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
164.402	Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.	A breach notification policy is in place in the event of a breach of ePHI.	Inquired of the CEO regarding breach notifications to determine that a breach notification policy was in place in the event of a breach of ePHI. Inspected the breach notification policies and procedures to determine that a breach notification policy was in place in the event of a breach of ePHI.	No exceptions noted. No exceptions noted.
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.

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 email address, website, or postal address.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not Applicable.	Not Applicable.
164.404 (c)(2)	The notification required by paragraph (a) of this section shall be written in plain language.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not Applicable.	Not Applicable.

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

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

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

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

BREACH NOTIFICATION				
Ref	**Regulation**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
164.408 (c)	For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in a manner specified on the HHS web site.	Not Applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.	Not Applicable.	Not Applicable.
164.410 (a)(1)	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	A breach notification policy is in place in the event of a breach of ePHI.	Inquired of the CEO regarding breach notifications to determine that a breach notification policy was in place in the event of a breach of ePHI.	No exceptions noted.
			Inspected the breach notification policies and procedures to determine that a breach notification policy was in place in the event of a breach of ePHI.	No exceptions noted.

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 CEO regarding breach notifications to determine that the entity acknowledged responsibility for notifying affected parties in the event of a breach of unsecured protected health information.	No exceptions noted.
			Inspected the information security policy regarding breach notifications to determine that the entity acknowledged responsibility for notifying affected parties in the event of a breach of unsecured protected health information.	No exceptions noted.
			Inspected the breach notification policies and procedures to determine that the entity acknowledged responsibility for notifying affected parties in the event of a breach of unsecured protected health information.	Testing of the control activity disclosed that there were no breaches of ePHI 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 60 calendar days after the discovery of the breach.	Inquired of the CEO regarding breach notifications to determine that the entity notified affected parties of a breach of ePHI no later than 60 calendar days after the discovery of the breach.	No exceptions noted.
			Inspected the breach notification policies and procedures and an example breach of ePHI to determine that the entity maintained procedures to guide personnel in notifying affected parties of a breach of ePHI no later than 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**
164.410 (c)(1)	The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired, used or disclosure during the breach.	The identification of each individual whose unsecured ePHI has been accessed during the breach is disclosed during notification procedures.	Inquired of the CEO regarding breaches of ePHI to determine that the identification of each individual whose unsecured ePHI had been accessed during the breach was disclosed during the notification procedures.	No exceptions noted.
			Inspected the breach notification policies and procedures and an example breach of ePHI to determine that the identification of each individual whose unsecured ePHI had been accessed during the breach was disclosed during notification procedures.	No exceptions noted.
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 CEO regarding breach notifications 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 policies and procedures and 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.	No exceptions noted.

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 maintains 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.	Inspected the breach notification policies and procedures to determine that the entity maintained procedures to guide personnel in refraining from, or delaying notification to the HHS personnel, the covered entity, or other required persons following the discovery of a breach of unsecured protected health information when required by law.	No exceptions noted.

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

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, CC4.1	Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance and conduct evaluation form for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	Testing of the control activities disclosed that performance evaluations were not performed for five of five current employees sampled.	Management recognizes that annual performance evaluations were not completed during the audit period. Since then, we've implemented a structured annual review process with documented completion tracking.
CC4.1, CC6.1, CC6.2, CC6.3	Logical access reviews are performed annually.	Inspected the completed access review for the in-scope systems to determine that logical access reviews were performed annually.	Testing of the control activities disclosed that logical access reviews were not performed within the review period. Subsequent testing disclosed that logical access reviews were performed after the review period.	Management has established a quarterly review cadence and automated reminders to ensure reviews are completed and documented on time.