A-LIGN

Med+Proctor

Type 2 SOC 2

2022

med+proctor

A-LIGN.COM

REPORT ON MED+PROCTOR'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY

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

March 1, 2022 to August 31, 2022

Table of Contents

SECTION 1

ASSERTION OF MED+PROCTOR MANAGEMENT

ASSERTION OF MED+PROCTOR MANAGEMENT

September 20, 2022

We have prepared the accompanying description of Med+Proctor's (or 'the Company') Health Data Services System titled "Med+Proctor's Description of Its Health Data Services System throughout the period March 1, 2022 to August 31, 2022" (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 Health Data Services System that may be useful when assessing the risks arising from interactions with Med+Proctor's system, particularly information about system controls that Med+Proctor 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 and 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*).

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

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

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

a. the description presents Med+Proctor's Health Data Services System that was designed and implemented throughout the period March 1, 2022 to August 31, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period March 1, 2022 to August 31, 2022, to provide reasonable assurance that Med+Proctor's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Med+Proctor's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period March 1, 2022 to August 31, 2022, to provide reasonable assurance that Med+Proctor's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Med+Proctor's controls operated effectively throughout that period.

Jeremy Jones

Jeremy Jones
Chief Executive Officer
Med+Proctor

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Med+Proctor

Scope

We have examined Med+Proctor's accompanying description of its Health Data Services System titled "Med+Proctor's Description of Its Health Data Services System throughout the period March 1, 2022 to August 31, 2022" (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 March 1, 2022 to August 31, 2022, to provide reasonable assurance that Med+Proctor's service commitments and system requirements were achieved based on the trust services criteria relevant to and 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*).

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

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

Service Organization's Responsibilities

Med+Proctor 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 Med+Proctor's service commitments and system requirements were achieved. Med+Proctor has provided the accompanying assertion titled "Assertion of Med+Proctor Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Med+Proctor is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

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

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

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

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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

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

Description of Tests of Controls

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

In our opinion, in all material respects,

a. the description presents Med+Proctor's Health Data Services System that was designed and implemented throughout the period March 1, 2022 to August 31, 2022, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period March 1, 2022 to August 31, 2022, to provide reasonable assurance that Med+Proctor's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Med+Proctor's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period March 1, 2022 to August 31, 2022, to provide reasonable assurance that Med+Proctor's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Med+Proctor'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 Med+Proctor, user entities of Med+Proctor's Health Data Services System during some or all of the period March 1, 2022 to August 31, 2022, business partners of Med+Proctor subject to risks arising from interactions with the Health Data Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

A-LIGN ASSURANCE

Tampa, Florida
September 20, 2022

SECTION 3

MED+PROCTOR’S DESCRIPTION OF ITS HEALTH DATA SERVICES SYSTEM THROUGHOUT THE PERIOD MARCH 1, 2022 TO AUGUST 31, 2022

OVERVIEW OF OPERATIONS

Company Background

Med+Proctor is a health care technology company headquartered in Nashville, Tennessee. The Company was founded in February 2014, as a Limited Liability Company in the state of Delaware. The Company has developed a technology platform that streamlines the process of collecting, verifying and storing critical medical data from incoming college students with a focus on electronic immunization verification.

The initial prototype was completed in May 2014. The Company used the prototype to test the market and gauge demand for an immunization verification solution. The Company called on several schools and completed numerous demonstrations. The Company concluded most schools were using a manual, paper-based process, and there was a need for an automated solution.

Description of Services Provided

Med+Proctor offers a web-based, platform-as-a-service (PaaS) technology solution for college student health centers. The platform streamlines the process of collecting, verifying and storing critical medical data from incoming college students with a focus on electronic immunization verification.

Med+Proctor’s solution solves many of the pain points found in a paper-based process. Med+Proctor uses a simple and user-friendly immunization form, which reduces common mistakes found on incomplete forms. Once uploaded, the technology digitizes the data on the form, which reduces the manual process of checking for legibility and completion. Student support is also provided, which reduces the burden of unwanted calls and e-mails from incoming students at the school health clinic.

At the same time, the Company collects other valuable data from students such as emergency contact, medical history, insurance, billing and more. Collecting this data electronically allows for more legible and accurate data. In addition, the product has an Application Programming Interface (API), which allows for seamless data integration with other systems of record at the school to eliminate the manual process of data entry.

The product has administrative features for allowing health center employees to easily manage the process from start to finish. The administrative dashboard allows schools to upload eligible users, track progress results in real-time, send out e-mail reminders to non-compliant students and view/upload/print student immunization forms.

In the event of a disease outbreak on campus, the platform can provide reports to view at-risk students. The report is generated using a database query, which identifies students who have not received certain immunizations, or requested exemptions for medical, religious, or other reasons. The school can use this tool to help prevent further spreading of an outbreak, and also quickly communicate to students and parents.

Med+Proctor is also a useful tool for students and parents in other ways. Automated e-mail reminders are a great tool to keep students and parents aware of deadlines. These messages contain useful tips on how to complete the process and avoid class registration holds. In addition, students have a lifetime subscription to Med+Proctor, so they can access immunization records in the future-like when they travel abroad, or attend graduate school.

Principal Service Commitments and System Requirements

Med+Proctor designs its processes and procedures related to web application to meet its objectives for its immunization verification services. Those objectives are based on the service commitments that Med+Proctor makes to user entities, the laws and regulations that govern the provision of Information Technology (IT) services, and the financial, operational, and compliance requirements that Med+Proctor has established for the services. The immunization verification services of Med+Proctor 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 Med+Proctor 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 Web Application 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 customer data both at rest and in transit

Med+Proctor establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Med+Proctor'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 IT.

Components of the System

Infrastructure

Primary infrastructure used to provide Med+Proctor's application system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Azure Application Services	Cloud	Hosting in-scope web application
Azure Structured Query Language (SQL)	Cloud	Hosting in-scope databases
Azure Virtual Network	Cloud	Hosting in-scope network
Azure DevOps	Cloud	Hosting source control

Software

Primary software used to provide Med+Proctor's application system includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
ASP.NET	Windows	Application web stack
SQL Server	Windows	Database server
Azure Active Directory (AD)	Windows	User account management

People

Med+Proctor has a staff of approximately 20 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, and human resources (HR). These individuals use the web application primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics as well as for Med+Proctor's user entities
- *Operations*. Staff that processes and communicates with students to have the users become fully compliant. They provide the direct day-to-day services
- *IT.* Help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support

Data

Data, as defined by Med+Proctor, constitutes the following:

- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

Output reports are available in electronic portable document format (PDF), comma-delimited value (.CVS) 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 e-mail, secure file transfer protocol (FTP), or secure websites-to transportation providers, treating facilities, and governments or managed care providers using Med+Proctor-developed websites or over connections secured by trusted security certificates. Med+Proctor uses Transport Layer Security (TLS) to encrypt e-mail 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. Teams are expected to adhere to the Med+Proctor policies and procedures that define how services should be delivered. These are located on the Company's Sharepoint site and can be accessed by any Med+Proctor team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by Azure. As such, Azure is responsible for the physical security controls for the in-scope service. Please refer to the “Subservice Organization” section below for detailed controls.

Logical Access

Med+Proctor 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, Med+Proctor implements monitoring of one or more of the responsibilities. Monitoring be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing quarterly reviews of access by role.

Employees and approved vendor personnel sign on to the Med+Proctor network using an AD 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 AD. Passwords conform to defined password standards and are enforced through parameter settings in the AD. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID’s ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the system from outside the Med+Proctor network are required to use a token-based two-factor authentication (2FA) system. Employees are issued tokens upon employment and return the token during their exit interview. Vendor personnel are not permitted to access the system from outside the Med+Proctor network.

Customer employees’ access the application’s services through the Internet using the TLS functionality of their web-browser. These customer employees supply a valid user ID and password to gain access to customer cloud resources. Passwords conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with Med+Proctor’s configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Customer employees may sign on to their systems using virtual server administration accounts. These administration accounts use a two-factor digital certificate-based authentication system.

Upon hire, employees are assigned to a position in the HR management system. 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 on a daily basis. This daily 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 access roles from IDs belonging to terminated employees.

On a quarterly basis, managers review roles assigned to their direct reports. Role lists are generated by security and distributed to the managers via the event management system. Managers review the lists and indicate the required changes in the event management record. The record is routed back to the security help desk for processing. The security help desk manager identifies any records not returned within two weeks and follows up with the manager. As part of this process, the CISO reviews employees with access to privileged roles and requests modifications through the event management system.

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.

Backup infrastructure is hosted and maintained by Azure. The backup infrastructure resides in a different availability zone than production infrastructure.

The ability to recall backup media is restricted to a certain group of users within Azure AD.

Computer Operations - Availability

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

Med+Proctor monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Med+Proctor 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:

- Cloud resource capacity
- Disk storage
- Network bandwidth

Med+Proctor 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 Med+Proctor system owners review proposed operating system patches to determine whether the patches are applied. Customers and Med+Proctor 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 Med+Proctor staff validate that patches have been installed and if applicable that reboots have been completed.

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

Change Control

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

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

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

Med+Proctor 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 Med+Proctor system owners review proposed operating system patches to determine whether the patches are applied. Customers and Med+Proctor 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. Med+Proctor staff validate that patches have been installed and if applicable that reboots have been completed.

Data Communications

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

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

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

Vulnerability scanning is performed by a third-party vendor on a quarterly basis in accordance with Med+Proctor’s policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Med+Proctor 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 Med+Proctor system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees are authenticated through the use of a token-based 2FA system.

Boundaries of the System

The scope of this report includes the Health Data Services System performed in the Nashville, Tennessee facilities.

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

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

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

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

Commitment to Competence

Med+Proctor'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

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

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

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

Organizational Structure and Assignment of Authority and Responsibility

Med+Proctor’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.

Med+Proctor’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

Med+Proctor’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. Med+Proctor’s HR policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgement forms for the employee handbook 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

Med+Proctor’s risk assessment process identifies and manages risks that could potentially affect Med+Proctor’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. Med+Proctor 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 Med+Proctor, 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

Med+Proctor 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. Med+Proctor 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 Med+Proctor's Web Application system; as well as the nature of the components of the system result in risks that the criteria will not be met. Med+Proctor 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, Med+Proctor'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 Med+Proctor's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, IT. At Med+Proctor, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

General updates to entity-wide security policies and procedures are usually communicated to the appropriate Med+Proctor personnel via e-mail messages.

Specific information systems used to support Med+Proctor's Health Data Services System 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. Med+Proctor'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

Med+Proctor'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 Med+Proctor’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 Med+Proctor’s personnel.

Reporting Deficiencies

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

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities 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.

Criteria Not Applicable to the System

All Common/Security criterion are applicable to the Med+Proctor Health Data Services System.

Subservice Organizations

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

Subservice Description of Services

Azure provides cloud hosting services, which includes implementing physical and environmental security controls to protect the housed in-scope systems.

Complementary Subservice Organization Controls

Med+Proctor’s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Med+Proctor’s services to be solely achieved by Med+Proctor’s control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Employee Referrals, Inc.

The following subservice organization controls should be implemented by Azure to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Security / Common Criteria	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

Med+Proctor's management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Med+Proctor performs monitoring of the subservice organization controls, including the following procedures:

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

COMPLEMENTARY USER ENTITY CONTROLS

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

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

1. User entities are responsible for understanding and complying with their contractual obligations to Med+Proctor.
2. User entities are responsible for notifying Med+Proctor 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 Med+Proctor 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 Med+Proctor services.
6. User entities are responsible for providing Med+Proctor with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Med+Proctor 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.

Control Activities Specified by the Service Organization

The applicable trust services criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Med+Proctor’s description of the system. Any applicable trust services criteria that are not addressed by control activities at Med+Proctor 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, RELATED CONTROLS, AND TESTS OF CONTROLS

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

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

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

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

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

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, directives, guidelines and the employee handbook.	Inspected the employee handbook, information security policies and procedures and the entity's SharePoint site to determine that core values were communicated from executive management to personnel through policies, directives, guidelines and the employee handbook.	No exceptions noted.
		An employee handbook is documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook was documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook.	Inspected the signed employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.
		Upon hire, personnel are required to complete a background check.	Inspected the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee 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**
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	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.	No exceptions noted.
		Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the sanction policies to determine that sanction policies, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the 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.
		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.
		Executive management maintains independence from those that operate the key controls within the environment.	Inspected the organizational chart and completed internal controls matrix to determine that executive management maintained independence from those that operate the key controls within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls within the environment.	Inspected the board meeting minutes to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the completed internal controls matrix to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.
			Inspected the board meeting minutes to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.	No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary.	Inspected the revision history of the organizational chart to determine that executive management reviewed the organizational chart annually and made updates to the organizational structure and lines of reporting, if necessary.	No exceptions noted.

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

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Control Environment</th></tr>
<tr><th>CC1.0</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>CC1.4</td><td>COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.</td><td>Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.</td><td>Inspected the employee performance checklist and the security training material 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.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Performance and conduct evaluations are performed for personnel on an annual basis.</td><td>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.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>The entity evaluates the competencies and experience of candidates prior to hiring.</td><td>Inspected the resume for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.</td><td>Inspected the job description for a sample of job roles and resume for a sample of new hires to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.</td><td>No exceptions noted.</td></tr>
</table>

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.	Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the training completion tracker and meeting invite for a sample of current employees to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No exceptions noted.
		Executive management has created a training program for its employees.	Inspected the security awareness training material to determine that executive management created a training program for its employees.	No exceptions noted.
		Upon hire, personnel are required to complete a background check.	Inspected the completed background check for a sample of new hires to determine that upon hire, personnel were required to complete a background check.	No exceptions noted.
		A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to acknowledge the employee handbook.	Inspected the signed employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee on an annual basis.	No exceptions noted.
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance checklist and the security training material to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	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.	No exceptions noted.
		Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.	Inspected the sanction policies to determine that sanction policies, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's SharePoint site.	Inspected the information security policies and procedures, job description for a sample of job roles and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes and made available to its personnel through the entity's SharePoint site.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inspected the edit check configurations to determine that edits checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
		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 diagrams to determine that data flow diagrams, process flowcharts, narratives and procedures manuals were documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data that entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the intrusion detection system (IDS) and 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.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		The entity's policies and procedures and employee handbook are made available to employees through the entity's SharePoint site.	Inspected the entity's SharePoint site to determine that the entity's policies and procedures and employee handbook were made available to employees through the entity's SharePoint site.	No exceptions noted.
		Upon hire, employees are required to complete information security and awareness training.	Inspected the training completion tracker and meeting invite for a sample of new hires to determine that upon hire, employees were required to complete information security and awareness training.	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**
		Current employees are required to complete information security and awareness training on an annual basis.	Inspected the training completion tracker and meeting invite for a sample of current employees to determine that current employees were required to complete information security and awareness training on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook.	Inspected the signed employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee on an annual basis.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook.	Inspected the signed employee handbook acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and made available to employees through the entity's SharePoint site.	Inspected the incident management policies and procedures and the entity's SharePoint site to determine that documented escalation procedures for reporting failures incidents, concerns and other complaints were in place and made available to employees through the entity's SharePoint site.	No exceptions noted.
		The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's SharePoint site.	Inspected the entity's SharePoint site to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's SharePoint site.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The entity's third-party agreement delineates the boundaries of the system and describes relevant system components.	Inspected the third-party agreement master template to determine that the entity’s third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.
			Inspected the executed 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 master template to determine that the entity's third-party agreement communicated the system commitments and requirements of third-parties.	No exceptions noted.
			Inspected the executed 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 master template to determine that the entity's third-party agreement outlined and communicated the terms, conditions and responsibilities of third-parties.	No exceptions noted.
			Inspected the executed 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.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the service level agreement master template to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the executed agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.	Inspected the organizational chart, employee performance checklist and the entity's documented objectives and strategies to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.
		Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART).	Inspected the entity's documented objectives and strategies to determine that executive management had documented objectives that were SMART.	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the risk assessment and management policies and procedures to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
			Inspected the completed risk assessment to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the employee performance checklist, 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 business plans, budget, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected the board meeting minutes to determine that entity strategies, objectives and budgets were assessed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk assessment and management policies and procedures to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the risk assessment and management policies and procedures to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.	Inspected the risk assessment and management policies and procedures to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.	Inspected the completed fraud 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.
		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 threats and vulnerabilities that arise from the use of IT.	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.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the completed risk assessment to determine that changes to the entity's systems, applications, technologies, and tools were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, IDS and IPS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the board meeting minutes to determine that on an annual basis, management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.
		Control self-assessments that include, but are not limited to, logical access reviews are performed on at least a quarterly basis.	Inquired of the Chief Executive Officer regarding backup restoration tests and user access reviews to determine that control self-assessments that included logical access reviews were performed on a quarterly basis.	No exceptions noted.
			Inspected the completed user access review report and backup restoration test for a sample of quarters to determine that control self-assessments that included logical access reviews were performed on a quarterly 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**
		Control self-assessments that include backup restoration tests are performed on an annual basis.	Inspected the completed backup restoration test to determine that control self-assessments that included backup restoration tests were performed on an annual basis.	No exceptions noted.
		Vulnerability scans are performed quarterly on the environment to identify control gaps and vulnerabilities.	Inspected the vulnerability scan results for a sample of quarters to determine that vulnerability scans were performed quarterly on the environment to identify control gaps and vulnerabilities.	No exceptions noted.
		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.	No exceptions noted.
		Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation report for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions.	Inquired of the Chief Executive Officer regarding and compliance assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the completed risk and compliance assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	Testing of the control activity disclosed that no vulnerabilities, deviations and control gaps occurred during the review period.
			Inspected the supporting incident ticket for a vulnerability identified from a vulnerability scan or penetration test to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were communicated to those parties responsible for taking corrective actions.	Testing of the control activity disclosed that no vulnerabilities, deviations and control gaps occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are documented, investigated, and addressed.	Inquired of the Chief Executive Officer regarding and compliance assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.
			Inspected the completed risk and compliance assessments to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	No exceptions noted.
			Inspected the supporting incident ticket for a vulnerability identified from a vulnerability scan or penetration test to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	Testing of the control activity disclosed that no vulnerabilities, deviations and control gaps occurred during the review period.
			Inspected the supporting incident ticket for a deviation identified from the tool used to monitor key systems, tools and applications for compliance to determine that vulnerabilities, deviations and control gaps identified from the risk and compliance assessments were documented, investigated and addressed.	Testing of the control activity disclosed that no vulnerabilities, deviations and control gaps occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	Inquired of the Chief Executive Officer regarding and compliance assessments to determine that controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the completed risk and compliance assessments to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the supporting incident ticket for a deviation identified from the tool used to monitor key systems, tools and applications for compliance to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	Testing of the control activity disclosed that no vulnerabilities, deviations and control gaps occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the supporting incident ticket for a vulnerability identified from a vulnerability scan or penetration test to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	Testing of the control activity disclosed that no vulnerabilities, deviations and control gaps occurred during the review period.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and completed internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the completed internal controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the completed internal controls matrix to determine that management incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Organizational and information security policies and procedures are documented and made available to employee's through the entity's SharePoint site.	Inspected the information security policies and procedures and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's SharePoint site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the completed internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.
		The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats	Inspected the completed internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to: • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Organizational and information security policies and procedures are documented and made available to employee's through the entity's SharePoint site.	Inspected the information security policies and procedures and the entity's SharePoint site to determine that organizational and information security policies and procedures were documented and made available to its personnel through the entity's SharePoint site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel.	Inspected the organizational and information security policies and procedures to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	No exceptions noted.
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the information security policies and procedures and completed internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.
		Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the completed internal controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Control Activities</th></tr>
<tr><th>CC5.0</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>Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.</td><td>Inspected the completed internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security, user access approval, and authentication policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
	Network (Azure AD)			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Network administrative access is restricted to user accounts accessible by the Chief Technology Officer.	Inquired of the Chief Technology Officer regarding privileged access to determine that network administrative access was restricted to user accounts accessible by the Chief Technology Officer.	No exceptions noted.
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to user accounts accessible by the Chief Technology Officer.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Networks are configured to enforce password requirements that include: • Password length • Complexity • 2FA	Inspected the network password settings to determine that networks were configured to enforce password requirements that included: • Password length • Complexity • 2FA	No exceptions noted.
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout settings to determine that network account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging settings and example network audit log extracts to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and reviewed as-needed.	Inquired of Chief Technology Officer to determine that network audit logs were maintained and reviewed as-needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected example network audit log extracts to determine that network audit logs were maintained and reviewed as-needed.	No exceptions noted.
	Database (Azure RDS)			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Database administrative access is restricted to user accounts accessible by the Chief Technology Officer.	Inquired of Chief Technology Officer to determine that database administrative access was restricted to user accounts accessible by the Chief Technology Officer.	No exceptions noted.
			Inspected the database administrator listing and access rights to determine that database administrative access was restricted to user accounts accessible by the Chief Technology Officer.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Databases are configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length • Complexity • 2FA	Inspected the database password settings to determine that database were configured to enforce password requirements that included: • Password history • Password age (minimum and maximum) • Password length • Complexity • 2FA	No exceptions noted.
		Database users are authenticated via individually-assigned user accounts and passwords.	Observed a user login to the database to determine that database users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the database account lockout settings to determine that database account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database audit logging settings are in place that include: • Policy changes • Privilege use • Process tracking • System events	Inspected the database audit logging settings and example database audit log extracts to determine that database audit logging configurations were in place that included: • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Database audit logs are maintained and reviewed as-needed.	Inquired of the Chief Technology Officer regarding data base audit logs to determine the database audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected example database audit log extracts to determine that database audit logs were maintained and reviewed as-needed.	No exceptions noted.
	Application (Med+Proctor)			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Application administrative access is restricted to user accounts accessible by the Chief Technology Officer.	Inquired of Chief Technology Officer to determine that application administrative access was restricted to user accounts accessible by the Chief Technology Officer.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the application administrator listing and access rights to determine that application administrative access was restricted to user accounts accessible by the Chief Technology Officer.	No exceptions noted.
		The application is configured to enforce password requirements that include: • Password history • Password age (minimum and maximum) • Password length • Complexity • 2FA	Inspected the application password settings to determine that application was configured to enforce password requirements that included: • Password history • Password age (minimum and maximum) • Password length • Complexity • 2FA	No exceptions noted.
		Application users are authenticated via individually-assigned user accounts and passwords.	Observed a user login to the application to determine that application users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Application audit policy settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the application audit logging settings and example application audit log extracts to determine that application audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Application audit logs are maintained and reviewed as-needed.	Inquired of the Chief Executive Officer regarding application audit logs to determine that application audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected example application audit log extracts to determine that application audit logs were maintained and reviewed as-needed.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Critical data is stored in encrypted format using software supporting the advanced encryption standard (AES).	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES.	No exceptions noted.
		Control self-assessments that include, but are not limited to, logical access reviews are performed on at least a quarterly basis.	Inquired of the Chief Executive Officer regarding backup restoration tests and user access reviews to determine that control self-assessments that included logical access reviews were performed on a quarterly basis.	No exceptions noted.
			Inspected the completed user access review report and backup restoration test for a sample of quarters to determine that control self-assessments that included logical access reviews were performed on a quarterly basis.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Chief Technology Officer regarding hiring procedures to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the candidate selection checklist, user access listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the candidate selection checklist, user access listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked for an employee as a component of the termination process.	Inquired of the Chief Technology Officer regarding termination procedures to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
			Inspected the termination timeline checklist, user access listings and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Control self-assessments that include, but are not limited to, logical access reviews are performed on at least a quarterly basis.	Inquired of the Chief Executive Officer regarding backup restoration tests and user access reviews to determine that control self-assessments that included logical access reviews were performed on a quarterly basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed user access review report and backup restoration test for a sample of quarters to determine that control self-assessments that included logical access reviews were performed on a quarterly basis.	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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security, user access approval, and authentication policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Chief Technology Officer regarding hiring procedures to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
			Inspected the candidate selection checklist, user access listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access to systems is revoked for an employee as a component of the termination process.	Inquired of the Chief Technology Officer regarding termination procedures to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
			Inspected the termination timeline checklist, user access listings and user access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Control self-assessments that include, but are not limited to, logical access reviews are performed on at least a quarterly basis.	Inquired of the Chief Executive Officer regarding backup restoration tests and user access reviews to determine that control self-assessments that included logical access reviews were performed on a quarterly basis.	No exceptions noted.
			Inspected the completed user access review report and backup restoration test for a sample of quarters to determine that control self-assessments that included logical access reviews were performed on a quarterly basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
	Network			
		Network user access is restricted via role-based security privileges defined within the access control system.	Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Database			
		Database user access is restricted via role-based security privileges defined within the access control system.	Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
	Application			
		Application user access is restricted via role-based security privileges defined within the access control system.	Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.5	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 retention policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		Data that is no longer required for business purposes is rendered unreadable.	Inquired of the Chief Technology Officer regarding data disposal to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the data retention policies and procedures to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the service ticket for a sample of requests to dispose data to determine that data that was no longer required for business purposes was rendered unreadable.	Testing of the control activity disclosed that no data disposals occurred during the review period.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		TLS is used for defined points of connectivity.	Inspected the encryption configurations and digital certificates to determine that TLS was used for defined points of connectivity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Chief Technology Officer to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the firewall rule sets to determine the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		IDS and IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS and IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDS and IPS configurations to determine that an IDS and IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS and IPS is configured to notify personnel upon intrusion detection and prevention.	Inspected the IDS and IPS log extract to determine that the IDS and IPS was configured to notify personnel upon intrusion detection and prevention.	No exceptions noted.
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the centralized antivirus configurations for a sample of workstations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on a daily basis.	Inspected the centralized antivirus settings to determine that the antivirus software was configured to scan workstations on a daily basis.	No exceptions noted.
		Critical data is stored in encrypted format using software supporting the AES.	Inspected encryption configurations for data at rest to determine that critical data was stored in encrypted format using AES.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Chief Technology Officer to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
		The entity secures its environment a using multi-layered defense approach that includes firewalls, an IDS and IPS, antivirus software and a DMZ.	Inspected the network diagram, IDS and IPS configurations, firewall rule sets, antivirus settings and DMZ settings to determine that the entity secured its environment a using multi-layered defense approach that included firewalls, an IDS and IPS, antivirus software and a DMZ.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		TLS is used for defined points of connectivity.	Inspected the encryption configurations and digital certificates to determine that TLS was used for defined points of connectivity.	No exceptions noted.
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall rule sets to determine the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		An IDS and IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS and IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
			Inspected the IDS and IPS configurations to determine that an IDS and IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS and IPS is configured to notify personnel upon intrusion detection and prevention.	Inspected the IDS and IPS log extract to determine that the IDS and IPS was configured to notify personnel upon intrusion detection and prevention.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected encryption configurations to determine that backup media was stored in an encrypted format.	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.	A warning notification appears when an employee attempts to download an application or software.	Inspected the warning notification received when an employee attempted to download an application or software to determine that a warning notification appeared when an employee attempted to download an application or software.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the centralized antivirus configurations for a sample of workstations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on a daily basis.	Inspected the centralized antivirus settings to determine that the antivirus software was configured to scan workstations on a daily basis.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall rule sets to determine the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security, computer and logging, 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity’s ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Vulnerability scans are performed quarterly on the environment to identify control gaps and vulnerabilities.	Inspected the vulnerability scan results for a sample of quarters to determine that vulnerability scans were performed quarterly on the environment to identify control gaps and vulnerabilities.	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, computer and logging, 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.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, IDS and IPS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		An IDS and IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram to determine that an IDS and IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the IDS and IPS configurations to determine that an IDS and IPS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS and IPS is configured to notify personnel upon intrusion detection and prevention.	Inspected the IDS and IPS log extract to determine that the IDS and IPS was configured to notify personnel upon intrusion detection and prevention.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
			Inspected the firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
			Inspected the firewall rule sets to determine the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the centralized antivirus configurations for a sample of workstations to determine that antivirus software was installed on workstations to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus settings to determine that the antivirus software provider pushed updates to the installed antivirus software as new updates/signatures were available.	No exceptions noted.
		The antivirus software is configured to scan workstations on a daily basis.	Inspected the centralized antivirus settings to determine that the antivirus software was configured to scan workstations on a daily basis.	No exceptions noted.
	Network (Azure AD)			
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout settings to determine that network account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network audit logging settings are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging settings and example network audit log extracts to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Network audit logs are maintained and reviewed as-needed.	Inquired of Chief Technology Officer to determine that network audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected example network audit log extracts to determine that network audit logs were maintained and reviewed as-needed.	No exceptions noted.
	Database (Azure RDS)			
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the database account lockout settings to determine that database account lockout settings were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database audit logging settings are in place that include: • Policy changes • Privilege use • Process tracking • System events	Inspected the database audit logging settings and example database audit log extracts to determine that database audit logging configurations were in place that included: • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Database audit logs are maintained and reviewed as-needed.	Inquired of the Chief Technology Officer regarding data base audit logs to determine the database audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected example database audit log extracts to determine that database audit logs were maintained and reviewed as-needed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Application (Med+Proctor)			
		Application audit policy settings are in place that include: - Account logon events - Account management - Directory Service Access - Logon events - Object access - Policy changes - Privilege use - Process tracking - System events	Inspected the application audit logging settings and example application audit log extracts to determine that application audit logging configurations were in place that included: - Account logon events - Account management - Directory Service Access - Logon events - Object access - Policy changes - Privilege use - Process tracking - System events	No exceptions noted.
		Application audit logs are maintained and reviewed as-needed.	Inquired of the Chief Executive Officer regarding application audit logs to determine that application audit logs were maintained and reviewed as-needed.	No exceptions noted.
			Inspected example application audit log extracts to determine that application audit logs were maintained and reviewed as-needed.	No exceptions noted.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.	Not applicable.	Not applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and breach response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident management policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Chief Technology Officer regarding incident resolution to determine that resolutions of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that resolutions of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that resolutions of incidents were documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that no significant security incidents occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Chief Technology Officer regarding incident resolution to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that no significant security incidents occurred during the review period.
		Identified incidents are reviewed, monitored and investigated by an incident response team.	Inquired of the Chief Technology Officer regarding incident resolution to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine that the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Testing of the control activity disclosed that no significant security incidents occurred during the review period.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and breach response policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inquired of the Chief Technology Officer regarding incident resolution to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the incident response policies and procedures to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Testing of the control activity disclosed that no significant security incidents occurred during the review period.
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inquired of the Chief Technology Officer regarding security incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	Testing of the control activity disclosed that no significant 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**
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the incident management and breach response policies and procedures to determine that documented incident response and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inquired of the Chief Technology Officer regarding incident resolution to determine that resolutions of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that resolutions of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that resolutions of incidents were documented within the ticket and communicated to affected users.	Testing of the control activity disclosed that no significant security incidents occurred during the review period.
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.	Inquired of the Chief Technology Officer regarding security incidents to determine that remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the incident response policies and procedures to determine that 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 activity disclosed that no significant security incidents occurred during the review period.
		Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Inquired of the Chief Technology Officer regarding security incidents to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.	Testing of the control activity disclosed that no significant security incidents occurred during the review period.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Change management requests are opened for incidents that require permanent fixes.	Inspected the systems development life cycle guidelines to determine that change management requests were required to be opened for incidents that required permanent fixes.	No exceptions noted.

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the systems development life cycle guidelines 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 systems development life cycle guidelines 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 notification for a system change to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
		Access to implement changes in the production environment is restricted to authorized IT personnel.	Inquired of the Chief Technology Officer regarding access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the list of users with access to deploy changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the supporting change ticket for a sample of system changes to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.
		Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.	Inspected the change control software configurations to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed.	No exceptions noted.
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate development, quality assurance and production environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.
		System change requests are documented and tracked in a ticketing system.	Inspected the supporting change ticket for a sample of system changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected the supporting change ticket for a sample of system changes to determine that system changes were tested prior to implementation and types of testing performed depended on the nature of the change.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the systems development life cycle guidelines to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.	Inspected the vendor management policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.	No exceptions noted.

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Management obtains and reviews attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation report for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
		A formal third-party risk assessment is performed on an annual basis to identify threats that could impair system commitments and requirements.	Inspected the vendor management policies and procedures to determine that a formal third-party risk assessment was performed on an annual basis to identify threats that could impair system commitments and requirements.	No exceptions noted.