A-LIGN

A-LIGN.com

Type 2 SOC 2

Prepared for:
ANS Group Ltd.

Year:
2025

REPORT ON ANS GROUP LTD.'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

August 1, 2024 to July 31, 2025

Table of Contents

SECTION 1

ASSERTION OF ANS GROUP LTD. MANAGEMENT

ASSERTION OF ANS GROUP LTD. MANAGEMENT

October 13, 2025

We have prepared the accompanying description of ANS Group Ltd.'s ('ANS' or 'the Company') Managed Service Solution System titled "ANS Group Ltd.'s Description of Its Managed Service Solution System throughout the period August 1, 2024 to July 31, 2025" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Managed Service Solution System that may be useful when assessing the risks arising from interactions with ANS' system, particularly information about system controls that ANS has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

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

a. the description presents ANS' Managed Service Solution System that was designed and implemented throughout the period August 1, 2024 to July 31, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period August 1, 2024 to July 31, 2025, to provide reasonable assurance that ANS' 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 ANS' controls throughout that period.
c. the controls stated in the description operated effectively throughout the period August 1, 2024 to July 31, 2025, to provide reasonable assurance that ANS' 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 ANS' controls operated effectively throughout that period.

Katie King
General Manager, Security
ANS Group Ltd.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: ANS Group Ltd.

Scope

We have examined ANS' accompanying description of its Managed Service Solution System titled "ANS Group Ltd.'s Description of Its Managed Service Solution System throughout the period August 1, 2024 to July 31, 2025" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period August 1, 2024 to July 31, 2025, to provide reasonable assurance that ANS' service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

ANS 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 ANS, to achieve ANS' service commitments and system requirements based on the applicable trust services criteria. The description presents ANS' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ANS' 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 ANS, to achieve ANS' service commitments and system requirements based on the applicable trust services criteria. The description presents ANS' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ANS' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The information included in Section 5, "Other Information Provided by the Service Organization," is presented by ANS management to provide additional information and is not a part of the description. Information about ANS's management's response to testing exceptions has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve ANS's service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

ANS 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 ANS' service commitments and system requirements were achieved. ANS has provided the accompanying assertion titled "Assertion of ANS Group Ltd. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. ANS 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 ANS' Managed Service Solution System that was designed and implemented throughout the period August 1, 2024 to July 31, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period August 1, 2024 to July 31, 2025, to provide reasonable assurance that ANS' 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 ANS' controls throughout that period.
c. the controls stated in the description operated effectively throughout the period August 1, 2024 to July 31, 2025, to provide reasonable assurance that ANS' 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 ANS' 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 ANS, user entities of ANS' Managed Service Solution System during some or all of the period August 1, 2024 to July 31, 2025, business partners of ANS subject to risks arising from interactions with the Managed Service Solution 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
October 13, 2025

SECTION 3

ANS GROUP LTD.'S DESCRIPTION OF ITS MANAGED SERVICE SOLUTION SYSTEM THROUGHOUT THE PERIOD AUGUST 1, 2024 TO JULY 31, 2025

OVERVIEW OF OPERATIONS

Company Background

ANS is a UK based company with a client base extending across the world. Its head office is based in Manchester, United Kingdom. ANS have been in existence since 1996 and slowly built up its client base within cloud hosting, in October 2019 ANS acquired Alithya, a business specializing in Dynamics. In 2021 UKFast merged with ANS Ltd another UK based cloud hosting provider based in Manchester, UKFast had been in existence since 1999, on merging with ANS Ltd the decision was taken to adopt ANS as the main company name and dissolve the name 'UKFast'.

On 2nd February 2017 UKFast acquired Secure Information Assurance (SIA) which added public sector clients to UKFast's client base. Following this UKFast also joined partnership with ClearCloud in July 2018, with the full integration of ClearCloud into ANS happening in 2021, ClearCloud allowed ANS to expand into offering further cloud-based services in partnership with Azure. In May 2020 UK Fast was taken over by Inflexion following their initial investment in the business in October 2019, ANS Ltd was also taken over by Inflexion in February 2021 and in October 2021 the decision was made to merge the 2 businesses and become ANS. ANS now adopt the historic UKFast and ANS Ltd.'s clients and services (ClearCloud and SIA included).

In December 2022, ANS acquired Preact, a leading Dynamics 365 partner, who help SMB's accelerate their digital transformation. This acquisition will support ANS in expanding within the Microsoft market and supplying new and existing ANS clients with a CRM system to suit their business needs. This acquisition sees Preact merge into ANS departments.

ANS provides managed hosting and colocation providers, supplying dedicated server hosting, critical application hosting, and cloud hosting solutions. ANS fully own, manage and operate its ISO-certified data centre complex, which offers over 30,000 sq. ft. of enterprise-grade facilities for co-locating customer's IT equipment. In addition, ANS offer a gold partnership with Microsoft and operate Azure solutions to their client base.

ANS hosting solutions are designed to help businesses grow, with 24/7/365 UK-based support and dedicated account management as standard.

Description of Services Provided

ANS hosting solutions are designed to help businesses grow, with 24/7/365 UK-based support and dedicated account management as standard. ANS has 5 sites that it operates from, which are required to continue as a business and provide support functionality, managed hosting, and consultation services to clients.

ANS provides MS Dynamics services to clients as a re-seller, providing managed services to clients via Dynamics. The main dynamics solution is held within the Azure DC's in the UK and is managed by Azure. ANS support in the creation of solutions via Azure and clients utilize MS Dynamics. Data held on these systems is the property and responsibility of the client.

Principal Service Commitments and System Requirements

ANS designs its processes and procedures related to Managed Service Solution to meet its objectives for its Managed Service Solution services. Those objectives are based on the service commitments that ANS makes to user entities, the laws and regulations that govern the provision of Managed Service Solution services, and the financial, operational, and compliance requirements that ANS has established for the services. The Managed Service Solution services of ANS 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 ANS 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 concepts within the fundamental designs of the Managed Service Solution 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.

Encryption technologies are used to protect customer data both at rest and in transit.

ANS establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in ANS' 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 Managed Service Solution.

Components of the System

Infrastructure

Primary infrastructure used to provide ANS' Managed Service Solution System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Microsoft Azure	Cloud Service Provider	Infrastructure provider for cloud computing and networking services

Software

Primary software used to provide ANS' Managed Service Solution System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
MS Dynamics	Dynamics	CRM systems

People

ANS are a team of 702 employees with around 250 working within Managed Services (MS). The MS team deal directly with clients and utilize Dynamics.

Data

ANS offers Managed Service Solution and does not manage any customer data.

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

Physical Security

AND Group facilities are protected by walls and fencing around the entire perimeter. Each facility has a designated reception area and security guard 24 hours per day. CCTV coverage around perimeter of building covers wide area and covers potential means of entry into the location. There is an automatic gate, monitored by CCTV. Entry is gained either by access controls from within the building activated by one of the data center staff or via swipe card if authorized entry. CCTV location on exterior of building, CCTV covers the front of the site and coverage around the building - no blind spots. Windows are on outside of building but are walled up behind, so no access can be gained through windows on ground floor. A 24x7 Physical Intrusion Monitoring (alarm system) is in place on exterior doors and is primed and on at all times. Racks that house customer data are locked with access to these racks restricted to certain engineers. The Data Centre Manager controls keys and access to the racks.

To gain access to the building a visitor access code is required, issued by the Account Manager, which is only valid for the period of the visit. To prevent entry into the facility, visitors have to provide their access code, name and the company they work for at the gate. Once through the gate, clients have to go to the reception, where they are required to provide Government-issued identification and a picture is taken for the visitors logs. The visitors are also provided with a Radio Frequency Identification (RFID) access card, allowing them access to only areas they require entry to. While in the building visitors are continually monitored by CCTV, as well as having their RFID cards monitored. Visitors are accompanied by a trained engineer who stays with them throughout the duration of their visit. At the end of the visit, visitors are required to visit the reception to hand back in their RFID access card(s). Visitors are then monitored to ensure they leave in a timely manner.

Part of the in-scope system and supporting infrastructure is hosted by Azure. As such, Azure is responsible for the physical security controls for the in-scope system. Refer to the 'Subservice Organizations' section below for controls managed by Azure.

Logical Access

ANS control logical access systems using Role-Based Access Control (RBAC). RBAC is controlled via Azure Active Directory (AAD), utilizing conditional access policies to dictate where users access resources from. Restricting access to geographical locations and devices where pertinent. Conditional access policies are in place for different types of user accounts which is dictated by RBAC. Within ANS, employees in AAD have access to different permissions depending on their job function. When employees move roles within the business, their AAD is updated, which means the policy is changed/applied to be in line with their new department.

ANS employees access the ANS environment via their ANS devices which are onboarded when an employee is recruited. Devices are controlled through Intune, which acts as an asset manager, with the correct type of tagging against resources. ANS internal systems department manage the relationship of assets and their owners, and the department they belong to. Which dictates what type of applications they can access from their devices.

ANS devices are encrypted using BitLocker and protected from physical malicious attacks. Users are required to utilize multiple factors to access their devices which again is controlled through conditional access. Password complexities meet industry standards as well as lock out policies and screen lock time frames.

ANS employees utilize the Office365 suite of products to conduct their jobs which enforce document versioning protection and control surrounding data transfers in and out of the tenant. These are controlled though Purview, and alerts are ingested into Sentinel.

For the ANS engineering team, for access into customer solutions, this is controlled through each individual customer solution, however ANS ensures that secure access methodologies are in place.

ANS engineers can only access customer solutions from the ANS office which requires Virtual Private Network (VPN) connectivity to the Cisco Firewalls. VPN access is linked to AAD and requires Two-Factor Authentication (2FA) authentication to access VPN with username and password.

Once connected to the VPN, ANS employees access customer solutions using Azure lighthouse which delegated permissions are granted through, to each customer solution.

ANS engineers access customers solutions via Azure Lighthouse controlled via Azure AD and conditional access. Automated reviews exist for the different levels of access via Lighthouse which are reviewed by the Internal Systems team and the team leaders of engineers who have levels of access.

Computer Operations - Backups

Backup infrastructure is physically secured in locked cabinets within the cloud service provider centers. The backup infrastructure resides on private networks logically secured from other networks.

The ability to recall backup media from the third-party off-site storage facility is restricted to authorized operations personnel.

Computer Operations - Availability

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

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

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

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

Change Control

ANS 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 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.

ANS 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 ANS system owners review proposed operating system patches to determine whether the patches are applied. Customers and ANS 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. ANS 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 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 ANS. 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 ANS policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by ANS. 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 ANS system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system through from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the Managed Service Solution System performed in the Manchester, United Kingdom facilities.

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

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 ANS' control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of ANS' 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

ANS' 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

ANS' 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.
- Management receive monthly updates on security and operations and quarterly security working groups are held with key stakeholders. This ensures areas are being escalated and communicated where needed.

Organizational Structure and Assignment of Authority and Responsibility

ANS' 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.

ANS' 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

ANS' 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. ANS' human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

ANS' risk assessment process identifies and manages risks that could potentially affect ANS' 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. ANS 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 ANS, 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

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

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

Specific information systems used to support ANS' Managed Service Solution 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. ANS' 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

ANS' 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 ANS' 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 ANS' personnel.

Reporting Deficiencies

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

Changes to the System Since the Last Review

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

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common/Security criteria were applicable to the ANS Managed Service Solution System.

Subservice Organizations

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

Subservice Description of Services

Azure provides cloud hosting services, which includes implementing physical security controls to protect in-scope systems. Controls include, but are not limited to, visitor sign-ins, use of badges for authorized personnel, monitoring and logging of physical access to the facilities, intrusion detection, physical environment management and third-party security testing.

Complementary Subservice Organization Controls

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

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

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established.
		Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.

ANS 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, ANS performs monitoring of the subservice organization controls, including the following procedures:

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

COMPLEMENTARY USER ENTITY CONTROLS

ANS' 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 ANS' services to be solely achieved by ANS control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of ANS'.

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 ANS.
2. User entities are responsible for notifying ANS 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 ANS 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 ANS services.

6. User entities are responsible for providing ANS with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying ANS 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 ANS' description of the system. Any applicable trust services criteria that are not addressed by control activities at ANS 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 ANS was limited to the Trust Services Criteria, related criteria and control activities specified by the management of ANS and did not encompass all aspects of ANS' 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, procedures, the code of conduct and the employee handbook.	Inspected the employee handbook, information security policies and procedures and the entity's SharePoint to determine that core values were communicated from executive management to personnel through policies, procedures, the code of conduct and the employee handbook.	No exceptions noted.
		An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Prior to employment, personnel are required to complete a background check.	Inspected the completed background check form for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inquired of the Head of Compliance regarding handbook acknowledgement to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
			Inspected the employee handbook to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	Testing of the control activity disclosed that the employee handbook and code of conduct were not acknowledged for 25 of 25 current employees sampled.
		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				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the escalation policies and procedure and the entity's website to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		Upon hire, personnel are required to sign a confidentiality agreement.	Inspected the signed non-disclosure agreement for a sample of new hires to determine that upon hire, personnel were required to sign a confidentiality agreement.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	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.
		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 defines and documents the skills and expertise needed among its members.	Inspected the executive management job descriptions to determine that executive management defined and documented the skills and expertise needed among its members.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management evaluates the skills and expertise of its members annually.	Inspected the performance evaluation form for a sample of executive management members to determine that executive management evaluated the skills and expertise of its members annually.	No exceptions noted.
		Executive management maintains independence from those that operate the key controls implemented within the environment.	Inspected the organizational chart and the internal controls matrix to determine that executive management maintained independence from those that operate the key controls implemented within the environment.	No exceptions noted.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management review meeting PowerPoint deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Executive management evaluates the skills and competencies of those that operate the internal controls implemented within the environment annually.	Inspected the performance evaluation form for a sample of current employees to determine that executive management evaluated the skills and competencies of those that operate the internal controls implemented within the environment annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the internal controls matrix and management review meeting PowerPoint deck to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		A third-party performs an independent assessment of the entity's controls environment annually to assess the effectiveness of internal controls implemented within the environment.	Inspected the entity's completed attestation ISO report to determine that a third-party performed an independent assessment of the entity's controls environment annually to assess the effectiveness of internal controls implemented within the environment.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.	Inspected the organizational chart and senior lead auditor, lead auditor, compliance assistant, and security compliance officer job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor risk management, compliance and audit activities.	No exceptions noted.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Executive management maintains independence from those that operate the key controls implemented within the environment.	Inspected the organizational chart and the internal controls matrix to determine that executive management maintained independence from those that operate the key controls implemented within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary.	Inspected the revision history of the organizational chart to determine that executive management reviewed the organizational chart annually and made updates to the organizational structure and lines of reporting, if necessary.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint 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.
		Executive management has established proper segregations of duties for key job functions and roles within the organization.	Inspected the organizational chart, the internal controls matrix, and job description for a sample of job roles to determine that executive management established proper segregations of duties for key job functions and roles within the organization.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system.	Inspected the job description for a sample of job roles to determine that roles and responsibilities defined in written job descriptions considered and addressed specific requirements relevant to the system.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Prior to employment, personnel are required to complete a background check.	Inspected the completed background check form for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance and conduct evaluations are performed for personnel on 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.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance evaluation policies and procedures and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		The entity evaluates the competencies and experience of candidates prior to hiring.	Inspected the interview notes for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity evaluates the competencies and experience of third-parties prior to working with them.	Inspected the vendor risk assessment for a sample of third-parties to determine that the entity evaluated the competencies and experience of third-parties prior to working with them.	No exceptions noted.
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring process.	Inspected the job description for a sample of job roles and interview note for a sample of new hires to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring process.	No exceptions noted.
		The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives.	Inspected the recruiting process and job opening postings to determine that the entity had a recruiting department that was responsible for attracting individuals with competencies and experience that aligned with the entity's goals and objectives.	No exceptions noted.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the Continued Professional Education (CPE) training tracker for a sample of current employees to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management has created a training program for its employees.	Inspected the training policies and procedures and information security and awareness training program materials to determine that executive management created a training program for its employees.	No exceptions noted.
		The entity has implemented a mentor program to develop its personnel.	Inspected the mentor program PowerPoint deck to determine that the entity created a mentor program for its employees.	No exceptions noted.
		Executive management tracks and monitors compliance with continued professional education (CPE) training requirements.	Inspected the CPE training tracker to determine that executive management tracked and monitored compliance with CPE training requirements.	No exceptions noted.
		As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations and performs disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	Inspected the employee performance evaluation policies and procedures to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations and performed disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	No exceptions noted.
		The entity assesses training needs on an annual basis.	Inspected the performance management policy to determine that the entity assessed the training needs 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**
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inquired of the Head of Compliance regarding handbook acknowledgement to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
			Inspected the employee handbook to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	Testing of the control activity disclosed that the employee handbook and code of conduct were not acknowledged for 25 of 25 current employees sampled.
		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.
		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 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**
		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.
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the employee performance evaluation policies and procedures and competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations and performs disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	Inspected the employee performance evaluation policies and procedures to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations and performed disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.
		Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.	Inquired of the Head of Compliance regarding edit checks to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
			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 diagram 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 entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the code repository configurations, IDS configurations, IPS configurations, encryption methods and configurations and VPN authentication configurations to determine that data entered into the system, processed by the system and output from the system was protected from unauthorized access.	No exceptions noted.
		Data entered into the system is reviewed for completeness and accuracy.	Inspected the review meeting minutes to determine that data entered into the system was reviewed for completeness and accuracy.	No exceptions noted.
		Data processed within the system is reviewed for completeness and accuracy annually.	Inspected the data review meeting minutes to determine that data processed within the system was reviewed for completeness and accuracy annually.	No exceptions noted.
		Data output from the system is reviewed for completeness and accuracy annually.	Inspected the data review meeting minutes to determine that data output from the system was reviewed for completeness and accuracy annually.	No exceptions noted.
		Data and information critical to the system is assessed annually for relevance and use.	Inspected the data criticality assessment meeting minutes to determine that data and information critical to the system was assessed annually for relevance and use.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data is only retained for as long as required to perform the required system functionality, service or use.	Inspected the data retention policies and procedures to determine that data was retained for only as long as required to perform the required system functionality, service or use.	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.	Core values are communicated from executive management to personnel through policies, procedures, the code of conduct and the employee handbook.	Inspected the employee handbook, information security policies and procedures and the entity's SharePoint to determine that core values were communicated from executive management to personnel through policies, procedures, the code of conduct and the employee handbook.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inquired of the Head of Compliance regarding handbook acknowledgement to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
			Inspected the employee handbook to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	Testing of the control activity disclosed that the employee handbook and code of conduct were not acknowledged for 25 of 25 current employees sampled.
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the escalation policies and procedure and the entity's website to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint 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.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the Continued Professional Education (CPE) training tracker for a sample of current employees to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.
		The entity's policies and procedures, code of conduct and employee handbook are made available to personnel through the entity's SharePoint site.	Observed the entity's SharePoint site to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to personnel through the entity's SharePoint site.	No exceptions noted.
			Inspected the entity's SharePoint site to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to personnel through the entity's SharePoint site.	No exceptions noted.
		Upon hire, personnel are required to complete information security awareness training.	Inspected the information security awareness training completion tracking tool for a sample of new hires to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.

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 awareness training annually.	Inspected the information security awareness training completion tracking tool for a sample of current employees to determine that current employees were required to complete information security awareness training annually.	No exceptions noted.
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the management review meeting PowerPoint deck to determine that executive management met annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	No exceptions noted.
		Changes to job roles and responsibilities are communicated to personnel through the entity's SharePoint site.	Inspected the entity's SharePoint site to determine that changes to job roles and responsibilities were communicated to personnel through the entity's SharePoint site.	No exceptions noted.
		Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place and made available to personnel through the entity's SharePoint site.	Inspected the incident response policies and procedures and the entity's SharePoint site to determine that documented escalation procedures for reporting system failures, incidents, concerns, and other complaints were in place and made available to personnel through the entity's SharePoint site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's SharePoint site.	Inspected the entity's SharePoint site to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's SharePoint site.	No exceptions noted.
		The information security policies and procedures that communicate the system commitments and requirements of external users are provided to external users prior to allowing them access to the system.	Inspected the information security policies and procedures to determine that the information security policies and procedures that communicated the system commitments and requirements of external users were provided to external users prior to allowing them access to the system.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.	Inspected the organizational chart and senior lead auditor, lead auditor, compliance assistant, and security compliance officer job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor risk management, compliance and audit activities.	No exceptions noted.
		Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

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

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 outlines and communicates the terms, conditions and responsibilities of third-parties.	Inspected the master third-party agreement template and third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated the terms, conditions and responsibilities of third-parties.	No exceptions noted.
		The entity's contractor agreement outlines and communicates the terms, conditions and responsibilities of external users.	Inspected the contractor agreement template to determine that the entity's contractor agreement outlined and communicated the terms, conditions and responsibilities of external users.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the customer agreement template and customer agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
		Changes to commitments, requirements and responsibilities are communicated to third-parties, external users, and customers via website notices.	Inspected the entity's website to determine that changes to commitments, requirements and responsibilities were communicated to third-parties, external users and customers via website notices.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management meets annually with operational management to discuss the results of assessments performed by third-parties.	Inspected the management review meeting PowerPoint deck to determine that executive management met annually with operational management to discuss the results of assessments performed by third-parties.	No exceptions noted.
		The entity communicates to external parties, vendors and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.	Inspected the master third-party agreement template to determine that the entity communicated to external parties, vendors and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.	No exceptions noted.
		Changes to commitments and requirements relating to confidentiality are communicated to third-parties, external users, and customers via website notices.	Inspected the entity's website to determine that changes to commitments and requirements relating to confidentiality were communicated to third-parties, external users and customers via website notices.	No exceptions noted.
		Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management review meeting PowerPoint deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.
		The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.	Inspected the organizational chart, employee performance evaluation policies and procedures and the entity's documented objectives and strategies to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART).	Inspected the entity's documented objectives and strategies to determine that executive management had documented objectives that were SMART.	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that executive management identified and assessed risks that could prevent the entity's objectives from being achieved.	No exceptions noted.
		Executive management reviews policies, procedures and other control documents for alignment to the entity's objectives on an annual basis.	Inspected the management review meeting PowerPoint deck to determine that executive management reviewed policies, procedures and other control documents for alignment to the entity's objectives on an annual basis.	No exceptions noted.
		Executive management reviews and addresses repeated control failures.	Inspected the management meeting reports and PowerPoint deck to determine that executive management reviewed and addressed control failures.	No exceptions noted.
		Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.

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**
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.	Inspected the organizational chart and senior lead auditor, lead auditor, compliance assistant, and security compliance officer job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor risk management, compliance and audit activities.	No exceptions noted.
		The entity has defined the desired level of performance and operation in order to achieve the established entity objectives.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that the entity defined the desired level of performance and operation in order to achieve the established entity objectives.	No exceptions noted.
		Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies.	Inspected the employee performance evaluation policies and procedures, the entity's documented objectives and strategies and the documented key performance indicators for operational and internal controls effectiveness to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies.	No exceptions noted.
		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.

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**
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected the management reports to determine that entity strategies, objectives and budgets were assessed on an annual basis.	No exceptions noted.
		The entity's internal controls framework is based on a recognized ISO framework.	Inspected the compliance reports to determine that the entity's internal controls framework was based on a recognized ISO framework.	No exceptions noted.
		The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures.	Inspected the internal controls matrix, policies and procedures related to the relevant statutory, regulatory, legislative and contractual requirements, and the current registry of relevant regulatory, statutory, legislative and contractual requirements to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Applicable law, regulation, standard and legislature requirements are identified and integrated into the entity's strategies and objectives.	Inspected the entity's documented objectives and strategies, policies and procedures related to the relevant statutory, regulatory, legislative and contractual requirements, and the current registry of relevant regulatory, statutory, legislative and contractual requirements to determine that applicable law, regulation, standard and legislature requirements were identified and integrated into the entity's strategies and objectives.	No exceptions noted.
		The entity undergoes compliance audits at least annually to show compliance to relevant laws, regulations and standards.	Inspected the entity's completed attestation ISO reports to determine that the entity underwent compliance audits at least annually to show compliance to relevant laws, regulations and standards.	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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures, completed risk assessment, and associated incident ticket for an example internal control that had failed to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
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.	A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.
		Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management 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 for each identified vulnerability	Inspected the risk assessment and management policies and procedures and 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 for each identified vulnerability	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Identified risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures, completed risk assessment, and associated incident ticket for an example internal control that had failed to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.
		As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that as part of the annual risk assessment, management reviewed the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT.	Inspected the completed fraud assessment to determine that as part of management's assessment of fraud risks, management considered threats and vulnerabilities that arise from the use of IT.	No exceptions noted.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management review meeting PowerPoint deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.
		Changes to the regulatory, economic and physical environment in which the entity operates are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that changes to the regulatory, economic and physical environment in which the entity operates were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Performance and conduct evaluations are performed for personnel on an annual basis.	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.
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management review meeting PowerPoint deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.

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**
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.	Inspected the organizational chart and senior lead auditor, lead auditor, compliance assistant, and security compliance officer job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor risk management, compliance and audit activities.	No exceptions noted.
		A formal risk assessment is performed on at least an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	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, code repository configurations, IDS configurations, 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.	Inspected the entity policies and procedures and management review meeting PowerPoint deck to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.
		On an annual basis, management reviews the controls implemented within the environment for compliance and operational effectiveness and identifies potential control gaps and weaknesses.	Inspected the internal controls matrix and the completed internal audit results to determine that on an annual basis, management reviewed the controls implemented within the environment for compliance and operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.
		A data backup restoration test is performed on an annual basis.	Inquired of the Head of Compliance regarding restoration testing to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
		Internal and external vulnerability scans are performed quarterly and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results and associated resolution documentation for a sample of quarters to determine that vulnerability scans were performed quarterly and remedial actions were taken where necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment, and identified vulnerabilities are addressed and tracked to resolution.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment, and identified vulnerabilities were addressed and tracked to resolution.	No exceptions noted.
		A third-party performs an independent assessment of the controls environment annually to assess the effectiveness of controls within the environment.	Inspected the entity's completed attestation ISO reports to determine that a third-party performed an independent assessment of the controls environment annually to assess the effectiveness of controls within the environment.	No exceptions noted.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
		Logical access reviews are performed annually.	Inquired of the Head of Compliance regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed access review for the in-scope systems to determine that logical access reviews were performed annually.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software and an example IDS and IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management review meeting PowerPoint deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.	Inspected the organizational chart and senior lead auditor, lead auditor, compliance assistant, and security compliance officer job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor risk management, compliance and audit activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures, completed risk assessment, and associated incident ticket for an example internal control that had failed to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.
		Senior management assesses the results of the compliance, control and risk assessments performed on the environment.	Inspected the management review meeting PowerPoint deck to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment.	No exceptions noted.
		Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	Inspected the management review meeting PowerPoint deck to determine that senior management was made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are communicated to those parties responsible for taking corrective actions.	Inspected the various assessments performed on the environment and supporting incident tickets for a sample of internal control failures/gaps, vulnerabilities identified from a vulnerability scan or penetration test, and deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
		Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are documented, investigated, and addressed.	Inspected the various assessments performed on the environment and supporting incident tickets for a sample of internal control failures/gaps, vulnerabilities identified from a vulnerability scan or penetration test, and deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were documented, investigated and addressed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment are addressed by those parties responsible for taking corrective actions.	Inspected the various assessments performed on the environment and supporting incident tickets for a sample of internal control failures/gaps, vulnerabilities identified from a vulnerability scan or penetration test, and deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that vulnerabilities, deviations and control failures/gaps identified from the various assessments performed on the environment were addressed by those parties responsible for taking corrective actions.	No exceptions noted.
		Management tracks whether vulnerabilities, deviations and control failures/gaps identified as part of the evaluations performed are addressed in a timely manner.	Inspected the incident management reports and PowerPoint deck and risk register to determine that management tracked whether vulnerabilities, deviations and control failures/gaps identified as part of the evaluations performed were addressed in a timely manner.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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, completed risk assessment, and associated incident ticket for an example internal control that had failed to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	Inspected the completed risk assessment to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	No exceptions noted.
		Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	Inspected the various assessments performed on the environment and supporting incident tickets for a sample of internal control failures/gaps, vulnerabilities identified from a vulnerability scan or penetration test, and deviations identified from the tool used to monitor key systems, tools and applications for compliance to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control failures/gaps identified as part of the various evaluations performed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Prior to the development and implementation of internal controls into the environment, management considers the complexity, nature, and scope of its operations.	Inspected the internal controls matrix and supporting materials and management reports and a PowerPoint deck to determine that prior to the development and implementation of internal controls into the environment, management considers the complexity, nature and scope of its operations.	No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the internal controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity and disaster recovery 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.
		An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the organizational chart, the internal controls matrix, and completed access review to determine that an analysis of incompatible operational duties was performed on at least an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.

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 incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Management has documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	Inspected the internal controls matrix to determine that management documented the relationship and linkage between business processes, the relevant technologies used to support the business processes, and the controls in place to help secure those business processes.	No exceptions noted.
		Management has documented the controls implemented around the entity's technology infrastructure.	Inspected the internal controls matrix to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	No exceptions noted.
		As part of the risk assessment process, the use of technology in business processes is evaluated by management.	Inspected the completed risk assessment to determine that as part of the risk assessment process, the use of technology in business processes was evaluated by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Authentication of access • Protecting the entity's assets from external threats	Inspected the internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to: • Restricting access rights to authorized users • Authentication of access • Protecting the entity's assets from external threats	No exceptions noted.
		Management has established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	Inspected the internal controls matrix to determine that management established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management review meeting PowerPoint deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint 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 Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Organizational and information security policies and procedures are documented and made available to personnel through the entity's SharePoint site.	Inspected the organizational and information security policies and procedures and the entity's SharePoint to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's SharePoint site.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor risk management, compliance and audit activities.	Inspected the organizational chart and senior lead auditor, lead auditor, compliance assistant, and security compliance officer job descriptions to determine that responsible parties were defined and assigned to coordinate and monitor risk management, compliance and audit activities.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel.	Inspected the organizational and information security policies and procedures to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	No exceptions noted.
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and the internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.
		Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the internal controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.
		Process owners and management operate the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and the internal controls matrix to determine that process owners and management operated the controls implemented within the entity's environment based on the frequency defined in the organizational and information security policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Process owners and management investigate and troubleshoot control failures.	Inspected the completed risk assessment and associated incident ticket for an example internal control that had failed to determine that process owners and management investigated and troubleshot control failures.	No exceptions noted.
		The effectiveness of the internal controls implemented within the environment is evaluated annually.	Inspected the management review meeting PowerPoint deck to determine that the effectiveness of the internal controls implemented within the environment was evaluated annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access 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.	An inventory of system assets and components is maintained to classify and manage the information assets.	Inspected the inventory listing of system assets and components to determine that an inventory of system assets and components was maintained to classify and manage the information assets.	No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Head of Compliance regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Network user access is restricted via role based security privileges defined within the access control system.	Inquired of the Head of Compliance regarding network access to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the network user listing and access rights to determine that network user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Network administrative access is restricted to authorized personnel.	Inquired of the Head of Compliance regarding administrative access to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to authorized personnel.	No exceptions noted.
		Network users are authenticated via individually-assigned user accounts and passwords.	Inspected the network user listing and password configurations to determine that network users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
		The network is configured to enforce password requirements that include: • Password history • Maximum password age • Password length • Complexity	Inspected the network password settings to determine that the network was configured to enforce password requirements that included: • Password history • Maximum password age • Password length • Complexity	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 account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold	Inspected the network account lockout settings to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Network audit logging configurations are in place that include: • Account logon events • Logon events • System events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Logon events • System events	No exceptions noted.
		Network audit logs are maintained for review when needed.	Inquired of the Head of Compliance regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.
			Inspected the example network audit log extract to determine that network audit logs were maintained for review when needed.	No exceptions noted.
		Production server user access is restricted via role based security privileges defined within the access control system.	Inquired of the Head of Compliance regarding production server access to determine that production server user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the production server user listing and access roles for production servers to determine that production server user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Production server administrative access is restricted to authorized personnel.	Inquired of the Head of Compliance regarding administrative access to determine that production server administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production server administrator listing and access roles for production servers to determine that production servers administrative access was restricted to authorized personnel.	No exceptions noted.
		Production server users are authenticated via individually-assigned user accounts and passwords.	Inspected the production server user listings and password configurations for production servers to determine that production servers 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**
		Production servers are configured to enforce password requirements that include: • Password history • Maximum password age • Password length • Complexity	Inspected the password configurations for a sample of production servers to determine that the production servers were configured to enforce password requirements that included: • Password history • Maximum password age • Password length • Complexity	No exceptions noted.
		Production server account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the account lockout configurations for a sample of production servers to determine that production server account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Production server audit logging configurations are in place that include: • Account logon events • Logon events • System events	Inspected the audit logging configurations for a sample of production servers and an example production server audit log extract to determine that production server audit logging configurations were in place that included: • Account logon events • Logon events • System events	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**
		Production server audit logs are maintained for review when needed.	Inquired of the Head of Compliance regarding production server audit logs to determine that production server audit logs were maintained for review when needed.	No exceptions noted.
			Inspected the example production server audit log extract to determine that production server audit logs were maintained for review when needed.	No exceptions noted.
		Production database user access is restricted via role based security privileges defined within the access control system.	Inquired of the Head of Compliance regarding production database access to determine that production databases user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the user listing and access roles for production databases to determine that production databases user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Production database administrative access is restricted to authorized personnel.	Inquired of the Head of Compliance regarding administrative access to determine that database administrative access was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the production database administrator listing and access roles for production databases to determine that production databases administrative access was restricted to authorized personnel.	No exceptions noted.
		Production database users are authenticated via individually-assigned user accounts and passwords.	Inspected the production database user listings and password configurations for production databases to determine that production databases users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		Production databases are configured to enforce password requirements that include: • Password history • Maximum password age • Password length • Complexity	Inspected the password configurations for production databases to determine that production databases were configured to enforce password requirements that included: • Password history • Maximum password age • Password length • Complexity	No exceptions noted.
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the account lockout configurations for a sample of production databases to determine that operating system account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.

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**
		Production database audit logging configurations are in place to log user activity and system events.	Inspected the production databases audit logging configurations and an example production database audit log extract to determine that production databases audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Production database audit logs are maintained for review when needed.	Inquired of the Head of Compliance regarding the production databases audit logs to determine that the production databases audit logs were maintained for review when needed.	No exceptions noted.
			Inspected the example production database audit log extract to determine that production databases audit logs were maintained for review when needed.	No exceptions noted.
		Production application user access is restricted via role based security privileges defined within the access control system.	Inquired of the Head of Compliance regarding production application access to determine that production application user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
			Inspected the production application user listing and access roles to determine that production application user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.

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**
		Production application administrative access is restricted to authorized personnel.	Inquired of the Head of Compliance regarding administrative access to determine that production application administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production application administrator listing and access roles to determine that production application administrative access was restricted to authorized personnel.	No exceptions noted.
		Production application users are authenticated via individually-assigned user accounts and passwords.	Inspected the production application user listing and password configurations to determine that production application users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		The production application is configured to enforce password requirements that include: • Password history • Maximum password age • Password length • Complexity	Inspected the production application password configurations to determine that applications were configured to enforce password requirements that included: • Password history • Maximum password age • Password length • Complexity	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**
		Production application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the production application account lockout configurations to determine that application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Production application audit logging configurations are in place to log user activity and system events.	Inspected the production application audit logging configurations and an example production application audit log extract to determine that production application audit logging configurations were in place to log user activity and system events.	No exceptions noted.
		Production application audit logs are maintained for review when needed.	Inquired of the Head of Compliance regarding application audit logs to determine that application audit logs were maintained for review when needed.	No exceptions noted.
			Inspected the example production application audit log extract to determine that production application audit logs were maintained for review when 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**
		VPN user access is restricted via role based security privileges defined within the access control system.	Inquired of the Head of Compliance regarding VPN access to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the VPN user listing and access rights to determine that VPN user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		The ability to administer VPN access is restricted to authorized personnel.	Inquired of the Head of Compliance regarding administrative access to the VPN to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
			Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to authorized personnel.	No exceptions noted.
		Users are authenticated via multi-factor authentication prior to being granted remote access to the environment.	Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inspected the VLANs configurations to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data coming into the environment is secured and monitored through the use of firewalls and an IDS and IPS.	Inspected the IDS and IPS configurations, firewall rule sets and the network diagram to determine that data coming into the environment was secured and monitored through the use of firewalls and an IDS and IPS.	No exceptions noted.
		Firewall rulesets are in place to isolate outside access and data from the entity's environment.	Inspected the firewall rulesets to determine that firewall rulesets were in place to isolate outside access and data from the entity's environment.	No exceptions noted.
		Server certificate-based authentication is used as part of the Secure Sockets Layer (SSL) / Transport Layer Security (TLS) encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the Advanced Encryption Standard (AES).	Inspected the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		Encryption keys are protected during generation, storage, use, and destruction.	Inquired of the Head of Compliance regarding the encryption keys to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the encryption policies and procedures to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
		Logical access reviews are performed annually.	Inquired of the Head of Compliance regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the completed access review for the in-scope systems to determine that logical access reviews were performed annually.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Head of Compliance regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, in-scope user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked from personnel as a component of the termination process.	Inquired of the Head of Compliance regarding the termination process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the termination procedures, in-scope user listings, and user access revocation checklist for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Head of Compliance regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Head of Compliance regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews are performed annually.	Inquired of the Head of Compliance regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the completed access review for the in-scope systems to determine that logical access reviews were performed annually.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Head of Compliance regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, in-scope user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked from personnel as a component of the termination process.	Inquired of the Head of Compliance regarding the termination process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the termination procedures, in-scope user listings, and user access revocation checklist for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Head of Compliance regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	An analysis of incompatible operational duties is performed on at least an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the organizational chart, the internal controls matrix, and completed access review to determine that an analysis of incompatible operational duties was performed on at least an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.	No exceptions noted.
		Privileged access to sensitive resources is restricted to authorized personnel.	Inquired of the Head of Compliance regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network, operating system, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Network user access is restricted via role based security privileges defined within the access control system.	Inquired of the Head of Compliance regarding network access to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the network user listing and access rights to determine that network user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production server user access is restricted via role based security privileges defined within the access control system.	Inquired of the Head of Compliance regarding production server access to determine that production server user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the production server user listing and access roles for production servers to determine that production server user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Production database user access is restricted via role based security privileges defined within the access control system.	Inquired of the Head of Compliance regarding production database access to determine that production databases user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the user listing and access roles for production databases to determine that production databases user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Production application user access is restricted via role based security privileges defined within the access control system.	Inquired of the Head of Compliance regarding production application access to determine that production application user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the production application user listing and access roles to determine that production application user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Logical access reviews are performed annually.	Inquired of the Head of Compliance regarding user access reviews to determine that logical access reviews were performed annually.	No exceptions noted.
			Inspected the completed access review for the in-scope systems to determine that logical access reviews were performed annually.	No exceptions noted.
		Logical access to systems is approved and granted to personnel as a component of the hiring process.	Inquired of the Head of Compliance regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.
			Inspected the hiring procedures, in-scope user listings, and user access request ticket for a sample of new hires to determine that logical access to systems was approved and granted to personnel 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 from personnel as a component of the termination process.	Inquired of the Head of Compliance regarding the termination process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the termination procedures, in-scope user listings, and user access revocation checklist for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Head of Compliance regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.

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**
CC6.4	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.	Logical access to systems is revoked from personnel as a component of the termination process.	Inquired of the Head of Compliance regarding the termination process to determine that logical access to systems was revoked as a component of the termination process.	No exceptions noted.
			Inspected the termination procedures, in-scope user listings, and user access revocation checklist for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		Policies and procedures are in place to guide personnel in physical security activities.	Inspected the physical security policies and procedures to determine that policies and procedures were in place to guide personnel in physical security activities.	No exceptions noted.
		A manned reception desk is in place to monitor and control access to the entrance of the office facility during standard business hours.	Observed the entrance to the facility to determine that a manned reception desk was in place to monitor and control access to the entrance of the office facility during standard business hours.	No exceptions noted.
			Inspected the Physical Security Policy to determine that a manned reception desk was in place to monitor and control access to the entrance of the office facility during standard business hours.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A badge access system controls access to and within the office facility.	Observed the presence of badge access points within the facility to determine that a badge access system controlled access to and within the facility.	No exceptions noted.
			Inspected the badge access listing and zone definitions to determine that a badge access system controlled access to and within the facility.	No exceptions noted.
		Personnel are assigned to predefined badge access security zones based on job responsibilities.	Inspected the badge access listing and zone definitions to determine that personnel were assigned to predefined badge access security zones based on job responsibilities.	No exceptions noted.
		The badge access system logs successful and failed physical access attempts. The logs can be pulled for review if necessary.	Inspected the badge access configurations and the badge access log for an example day to determine that the badge access system logged successful and failed access attempts and logs could be pulled for review if necessary.	No exceptions noted.
		Privileged access to the badge access system is restricted to authorized personnel.	Inquired of the Head of Compliance regarding privileged access to determine that privileged access to the badge access system was restricted to authorized personnel.	No exceptions noted.
			Inspected the badge access administrator listing to determine that privileged access to the badge access system was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A video surveillance system is in place with footage retained for 100 days.	Observed the video surveillance system throughout the office facility to determine that a video surveillance system was in place with footage retained for 100 days.	No exceptions noted.
			Inspected the video surveillance system configurations and oldest retained video surveillance footage to determine that a video surveillance system was in place with footage retained for 100 days.	No exceptions noted.
		Visitors to the office facility are required to be escorted by an authorized employee.	Observed the overall visitor process to determine that visitors to the office facility were required to be escorted by an authorized employee.	No exceptions noted.
			Inspected the physical security policies and procedures to determine that visitors to the office facility were required to be escorted by an authorized employee.	No exceptions noted.
		Visitors to the office facility are required to sign a visitor log prior upon arrival.	Inspected the visitor log for an example month to determine that visitors to the facility were required to sign a visitor log prior upon arrival.	No exceptions noted.
		Physical access is reviewed on at least an annual basis.	Inspected the physical access review to determine that physical access to was reviewed on at least an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Part of this criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization.	Not applicable.	Not applicable.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.	Inspected the data disposal and destruction policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		A third-party purges data stored on backup drivers per a defined schedule.	Inspected the data disposal vendor's contract to determine that a third-party purged data stored on backup drivers per a defined schedule.	No exceptions noted.
		Data that is no longer required is disposed of and rendered unreadable to meet the entity's objectives.	Inspected the data disposal and destruction policies and procedures and destruction certificate for a sample of requests to purge a system to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	VPN user access is restricted via role based security privileges defined within the access control system.	Inquired of the Head of Compliance regarding VPN access to determine that VPN user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the VPN user listing and access rights to determine that VPN user access was restricted via role based security privileges defined within the access control system.	No exceptions noted.
		Users are authenticated via multi-factor authentication prior to being granted remote access to the environment.	Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
		Firewall rulesets are in place to isolate outside access and data from the entity's environment.	Inspected the firewall rulesets to determine that firewall rulesets were in place to isolate outside access and data from the entity's environment.	No exceptions noted.
		Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the AES.	Inspected the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		VPN, SSL/TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN, SSL/TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Head of Compliance regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access rights to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram and firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS and IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and 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 configurations, an example IDS and IPS log extract and alert notification 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 and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console and antivirus configurations for a sample of workstations and servers to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus software dashboard console, antivirus software configurations for a sample of workstations and servers and an example antivirus update log 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 and servers in real-time.	Inspected the antivirus software dashboard console and antivirus software configurations to determine that the antivirus software was configured to scan workstations and servers in real-time.	No exceptions noted.
		Use of removable media is prohibited by policy and system configuration except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy and system configuration except when authorized by management.	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.	Users are authenticated via multi-factor authentication prior to being granted remote access to the environment.	Inspected the VPN authentication settings to determine that VPN users were authenticated via multi-factor authentication prior to being granted remote access to the system.	No exceptions noted.
		Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and to determine that server certificate-based authentication was used as part of the SSL/TLS encryption with a trusted certificate authority.	No exceptions noted.
		Passwords and production data is stored in an encrypted format using software supporting the AES.	Inspected the encryption configurations for data at rest to determine that passwords and production data was stored in an encrypted format using software supporting the AES.	No exceptions noted.
		NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		VPN, SSL/TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations, VPN authentication configurations and digital certificates to determine that VPN, SSL/TLS and other encryption technologies were 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**
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Head of Compliance regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the database user listing and access 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 and firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS and IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and 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 configurations, an example IDS and IPS log extract and alert notification to determine that the IDS and IPS was configured to notify personnel upon intrusion detection and prevention.	No exceptions noted.
		Use of removable media is prohibited by policy and system configuration except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy and system configuration except when authorized by management.	No exceptions noted.
		The ability to restore backups is restricted to authorized personnel.	Inquired of the Head of Compliance regarding restoring backed up data to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the listing of users with the ability to restore backups to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.
		Backup data is stored in an encrypted format.	Inspected the encryption configurations for backup data to determine that backup data was stored in an encrypted format.	No exceptions noted.
		Mobile devices are protected through the use of secured, encrypted connections.	Inspected the encryption configurations for laptops to determine that mobile devices were protected through the use of secured, encrypted connections.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	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, code repository configurations, IDS configurations, 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.

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 and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console and antivirus configurations for a sample of workstations and servers to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus software dashboard console, antivirus software configurations for a sample of workstations and servers and an example antivirus update log 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 and servers in real-time.	Inspected the antivirus software dashboard console and antivirus software configurations to determine that the antivirus software was configured to scan workstations and servers in real-time.	No exceptions noted.
		The ability to install applications and software on workstations is restricted to authorized personnel.	Inquired of the Head of Compliance regarding the applications and software to determine that the ability to install applications and software on workstations was restricted to authorized personnel.	No exceptions noted.

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 denial notification to determine that a warning notification appeared when an employee attempted to download an application or software.	No exceptions noted.
		The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Head of Compliance regarding the ability to migrate changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
			Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
		Code repository is utilized to help detect unauthorized changes within the production environment.	Inspected the code repository configurations to determine that Code repository was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		The Code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from the Code repository to determine that the Code repository was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software and an example IDS and IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, code repository configurations, IDS configurations, 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.
		Internal and external vulnerability scans are performed quarterly and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results and associated resolution documentation for a sample of quarters to determine that vulnerability scans were performed quarterly and remedial actions were taken where necessary.	No exceptions noted.
		A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment, and identified vulnerabilities are addressed and tracked to resolution.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing annually to identify and exploit vulnerabilities identified within the environment, and identified vulnerabilities were addressed and tracked to resolution.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram and firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS and IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and 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 configurations, an example IDS and IPS log extract and alert notification to determine that the IDS and IPS was configured to notify personnel upon intrusion detection and prevention.	No exceptions noted.
		Use of removable media is prohibited by policy and system configuration except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy and system configuration except when authorized by management.	No exceptions noted.
		Code repository is utilized to help detect unauthorized changes within the production environment.	Inspected the code repository configurations to determine that Code repository was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from the Code repository to determine that the Code repository was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		Management defined configuration standards in the information security policies and procedures.	Inspected the information security policies and procedures to determine that management defined configuration standards in the information security policies and procedures.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software and an example IDS and IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.

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.	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, code repository configurations, IDS configurations, 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.
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold	Inspected the network account lockout settings to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold	No exceptions noted.
		Network audit logging configurations are in place that include: • Account logon events • Logon events • System events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Logon events • System events	No exceptions noted.
		Network audit logs are maintained for review when needed.	Inquired of the Head of Compliance regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.

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

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the example production application audit log extract to determine that production application audit logs were maintained for review when needed.	No exceptions noted.
		The badge access system logs successful and failed physical access attempts. The logs can be pulled for review if necessary.	Inspected the badge access configurations and the badge access log for an example day to determine that the badge access system logged successful and failed access attempts and logs could be pulled for review if necessary.	No exceptions noted.
		A video surveillance system is in place with footage retained for 100 days.	Observed the video surveillance system throughout the office facility to determine that a video surveillance system was in place with footage retained for 100 days.	No exceptions noted.
			Inspected the video surveillance system configurations and oldest retained video surveillance footage to determine that a video surveillance system was in place with footage retained for 100 days.	No exceptions noted.
		Visitors to the office facility are required to sign a visitor log prior upon arrival.	Inspected the visitor log for an example month to determine that visitors to the facility were required to sign a visitor log prior upon arrival.	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 and firewall rule sets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rule sets to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS and IPS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and 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 configurations, an example IDS and IPS log extract and alert notification 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 and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the antivirus software dashboard console and antivirus configurations for a sample of workstations and servers to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the antivirus software dashboard console, antivirus software configurations for a sample of workstations and servers and an example antivirus update log 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 and servers in real-time.	Inspected the antivirus software dashboard console and antivirus software configurations to determine that the antivirus software was configured to scan workstations and servers in real-time.	No exceptions noted.
		Use of removable media is prohibited by policy and system configuration except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy and system configuration except when authorized by management.	No exceptions noted.
		Code repository is utilized to help detect unauthorized changes within the production environment.	Inspected the code repository configurations to determine that Code repository was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The Code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from the Code repository to determine that the Code repository was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software and an example IDS and IPS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		CCTV cameras monitor physical access to the entity's office facilities and visitor access to the office facilities require the visitor to sign a visitor log prior upon arrival.	Observed the CCTV cameras in place at the entity's office facilities to determine that CCTV cameras monitored physical access to the entity's office facilities and visitor access to the office facilities required the visitor to sign a visitor log prior upon arrival.	No exceptions noted.
			Inspected the visitor log for an example month to determine that CCTV cameras monitored physical access to the entity's facilities and visitor access to the facility and server room required the visitor to sign a visitor log prior upon arrival.	No exceptions noted.
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the meeting minutes to determine that management reviewed reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.
		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 escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident response policies and procedures to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents is documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inspected the supporting incident ticket for a sample of critical security incidents to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
		Identified incidents are reviewed, monitored and investigated by an incident response team.	Inspected the supporting incident ticket for a sample of incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
		Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inspected the incident ticket for a sample of critical security incidents that resulted in unauthorized disclosure of personal information to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and communicated to the affected users.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident management and escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the meeting minutes to determine that management reviewed reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident response policies and procedures to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents is documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents was documented within the ticket and communicated to affected users.	No exceptions noted.
		Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	Inspected the supporting incident ticket for a sample of incidents to determine that incidents were documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inspected the supporting incident ticket for a sample of critical security incidents to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
		Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the incident response policies and procedures to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented.	No exceptions noted.
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inspected the supporting incident ticket for a sample of incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Critical security incidents that result in a service/business operation disruption are communicated to those affected through creation of an incident ticket.	Inspected the security incident analysis for a sample of critical security incidents that resulted in a service/business operation disruption to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through creation of an incident ticket.	No exceptions noted.
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine that the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		The risks associated with identified vulnerabilities are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the supporting incident ticket (or e-mails) for a vulnerability identified from a vulnerability scan or penetration test and completed risk assessment to determine that the risks associated with identified vulnerabilities were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	A data backup restoration test is performed on an annual basis.	Inquired of the Head of Compliance regarding restoration testing to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the 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.
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the meeting minutes to determine that management reviewed reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inspected the supporting incident ticket for a sample of critical security incidents to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Change management requests are opened for incidents that require permanent fixes.	Inspected the change management policies and procedures and the change ticket for an example incident that required a permanent fix to determine that change management requests were required to be opened for incidents that required permanent fixes.	No exceptions noted.
		The entity restores system operations for incidents impacting the environment through activities that include, but are not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	Inspected the information security, incident, and change management policies and procedures, and the system build guides for critical systems to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.

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 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.	The ability to migrate changes into the production environment is restricted to authorized and appropriate users.	Inquired of the Head of Compliance regarding the ability to migrate changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
			Inspected the list of users with the ability to implement changes into the production environment to determine that the ability to migrate changes into the production environment was restricted to authorized and appropriate users.	No exceptions noted.
		Code repository is utilized to help detect unauthorized changes within the production environment.	Inspected the code repository configurations to determine that Code repository was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		The Code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.	Inspected the code repository notification configurations and an example alert generated from the Code repository to determine that the Code repository was configured to notify IT personnel via e-mail alert when a change to the production application code files was detected.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Authorization of change requests - Owner or business unit manager • Development - Application Design and Support Department • Testing - Quality Assurance Department • Implementation - Software Change Management Group	Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests - Owner or business unit manager • Development - Application Design and Support Department • Testing - Quality Assurance Department • Implementation - Software Change Management Group	No exceptions noted.
		System changes are communicated to both affected internal and external users.	Inspected the change tickets and e-mails to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System changes are authorized and approved by management prior to implementation.	Inspected the supporting change ticket for a sample of infrastructure, operating system, database and application changes to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.
		Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.	Inspected the change control software settings to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed.	No exceptions noted.
		System patches/security updates follow the standard change management process.	Inspected the patch management policies and procedures to determine that system patches/security updates follow the standard patch management process.	No exceptions noted.
		System patches/security updates are performed on a configured schedule.	Inspected the system patching configurations and an example patching job to determine that system patches/security updates were performed on a configured schedule.	No exceptions noted.
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate development, QA and production environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		System change requests are documented and tracked in a ticketing system.	Inspected the supporting change ticket for a sample of infrastructure, operating system, database and application changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.
		Back out procedures are documented to allow for rollback of application changes when changes impaired system operations.	Inspected the rollback capabilities to determine that back out procedures were documented to allow for rollback of application changes when changes impaired system operation.	No exceptions noted.
		A code/peer review is systematically required prior to deploying the PR into the production environment.	Inspected the supporting change ticket for a sample of infrastructure, database and application changes to determine that a code/peer review was systematically required prior to deploying the PR into the production environment.	No exceptions noted.
		System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected the supporting change ticket for a sample of infrastructure, operating system, database and application changes to determine that system changes were tested prior to implementation, and that types of testing performed depended on the nature of the change.	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 implemented for remediating incidents follow the standard change management process.	Inspected the change management policies and procedures and supporting change ticket for a sample of incidents to determine that system changes implemented for remediating incidents followed the standard change management process.	No exceptions noted.
		Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.	Inspected the information security policies and procedures to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the 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 and completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the risk assessment and management policies and procedures and completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures, completed risk assessment, and associated incident ticket for an example internal control that had failed to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
		Documented policies and procedures are in place to guide personnel in performing risk assessment and risk mitigation activities.	Inspected the risk assessment and management policies and procedures to determine that documented policies and procedures were in place to guide personnel in performing risk assessment and risk mitigation activities.	No exceptions noted.

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 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.
		Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the 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.

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**
		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 and completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has established exception handling procedures for services provided by third-parties.	Inspected the third-party and vendor policies and procedures to determine that management established exception handling procedures for services provided by third-parties.	No exceptions noted.
		The entity has documented procedures for addressing issues identified with third-parties.	Inspected the third-party and vendor policies and procedures to determine that the entity documented procedures for addressing issues identified with third-parties.	No exceptions noted.
		The entity has documented procedures for terminating third-party relationships.	Inspected the third-party and vendor policies and procedures to determine that the entity documented procedures for terminating third-party relationships.	No exceptions noted.
		The entity's third-party agreement outlines and communicates confidentiality commitments and requirements.	Inspected the master third-party agreement template and third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated confidentiality commitments and requirements.	No exceptions noted.
		Management assesses the compliance of confidential commitments and requirements of third-parties at least annually.	Inspected the evaluation forms to determine that management assessed the compliance of confidential commitments and requirements of third-parties at least annually.	No exceptions noted.

SECTION 5

OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Control Point	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response
CC1.1, CC1.5, CC2.2	Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	Testing of the control activity disclosed that the employee handbook and code of conduct were not acknowledged for 25 of 25 current employees sampled.	ANS request employees to complete this as part of the PDR annually, gaps often occur due to sickness and maternity.