A-LIGN

A-LIGN.com

Type 2 SOC 2

Prepared for:
ATPI Limited

Date:
2025

ATPI

REPORT ON ATPI LIMITED'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

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

December 1, 2024 to February 28, 2025

Table of Contents

SECTION 1

ASSERTION OF ATPI LIMITED MANAGEMENT

ASSERTION OF ATPI LIMITED MANAGEMENT

May 21, 2025

We have prepared the accompanying description of ATPI Limited's ('ATPI' or 'the Company') Travel Management Services Booking System titled "ATPI Limited's Description of Its Travel Management Services Booking System throughout the period December 1, 2024 to February 28, 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 Travel Management Services Booking System that may be useful when assessing the risks arising from interactions with ATPI's system, particularly information about system controls that ATPI 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 and Availability (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*).

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

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

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

a. the description presents ATPI's Travel Management Services Booking System that was designed and implemented throughout the period December 1, 2024 to February 28, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period December 1, 2024 to February 28, 2025, to provide reasonable assurance that ATPI's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of ATPI's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period December 1, 2024 to February 28, 2025, to provide reasonable assurance that ATPI's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of ATPI's controls operated effectively throughout that period.

Jeroen van Hest
Chief of Staff
ATPI Limited

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: ATPI Limited

Scope

We have examined ATPI's accompanying description of its Travel Management Services Booking System titled "ATPI Limited's Description of Its Travel Management Services Booking System throughout the period December 1, 2024 to February 28, 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 December 1, 2024 to February 28, 2025, to provide reasonable assurance that ATPI's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (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*).

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

The information included in Section 5, "Other Information Provided by the Service Organization," is presented by ATPI management to provide additional information and is not a part of the description. Information about ATPI'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 ATPI's service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

ATPI 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 ATPI's service commitments and system requirements were achieved. ATPI has provided the accompanying assertion titled "Assertion of ATPI Limited Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. ATPI 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 ATPI's Travel Management Services Booking System that was designed and implemented throughout the period December 1, 2024 to February 28, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period December 1, 2024 to February 28, 2025, to provide reasonable assurance that ATPI's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of ATPI's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period December 1, 2024 to February 28, 2025, to provide reasonable assurance that ATPI's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of ATPI's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4*,* is intended solely for the information and use of ATPI, user entities of ATPI's Travel Management Services Booking System during some or all of the period December 1, 2024 to February 28, 2025, business partners of ATPI subject to risks arising from interactions with the Travel Management Services Booking 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
May 21, 2025

SECTION 3

ATPI LIMITED'S DESCRIPTION OF ITS TRAVEL MANAGEMENT SERVICES BOOKING SYSTEM THROUGHOUT THE PERIOD DECEMBER 1, 2024 TO FEBRUARY 28, 2025

OVERVIEW OF OPERATIONS

Company Background

ATPI Group was formed in 2002 by the joining forces of various separate trading companies in the UK and Netherlands. The founding of one of these original trading companies (Instone) dates back to 1919. Since then, ATPI has gone on to expand its network across the globe. ATPI is a Travel Management Company providing specialized travel services in multiple areas including Corporate Travel; Marine Travel; Energy Travel; Sports Travel; Yacht Travel; Mining Travel; and Events. ATPI provides Global and Gateway Travel Solutions with offices worldwide. The HQ is based in Manchester in the UK.

Description of Services Provided

ATPI provides Travel Management for clients worldwide. Utilizing multiple in-house bespoke and third-party products to ensure the company meets the clients' requirements. ATPI book various travel and accommodation for clients, manage and maintain these bookings, from request through to invoice and provide detailed Management Information reports.

Client requirements vary from industry to industry and not all clients use the same products. ATPI uses and provides products that can carry out the following tasks:

- Fulfilment of travel requests (including self-online booking):
    - Flights
    - Accommodation
    - Rail / Ferry
    - Car Hire
    - VISA Services
    - Events Organisation
    - Other ancillary services as required
- Alerts to monitor and assist travelers
- Enabling clients' self-access to travel data
- Industry Bespoke travel management products (e.g. Crew Hub)
- CO2 monitoring, reporting and offset
- Control of travel expenses
- Traveler authorization
- Traveler tracking
- Invoicing
- Reconciliation
- Reporting
- Managing complaints

Flights are the most requested form of travel: Requests are received via e-mail or telephone (unless an online self-booking tool has been used) and the travel consultant searches for appropriate flights for the date and route requested. Clients have different SLAs but generally responses are provided within two hours with a minimum of three options for travel (if available). Upon confirmation of the required travel, authorization is received from the client and the reservation made. Reservations are ticketed and sent to the requestor.

The information is sent internally to the mid and back office to ensure the client's required information has been obtained (e.g. client's PO number) and processed for invoicing. This information is also used via a reporting system to provide regular reports to the client as agreed.

Dealing with large amounts of personal data (required for the fulfilment of travel arrangements) and protecting the commercially sensitive ATPI data involves ensuring the security of various systems. The transfer of sensitive data (e.g. Credit card details, passport information) is carried out via a PCI Portal which ensures security. Inbound / Outbound e-mails are blocked where they seem to contain credit card details. ATPI are currently working on including blocking passport information too.

These tasks are carried out by the Security Operations and IT Teams.

Information is shared with user entities by telephone, fax, secure electronic exchange: FTP (file transfer protocol), e-mail, EDI (electronic data interchange), and secured websites.

Principal Service Commitments and System Requirements

As a Global Company, ATPI creates its overall procedures to meet the requirements of the ISO certification that is in place and show adherence to the laws, regulations, insurance and other compliance aspects that impact the business as a whole. Local and Departmental objectives are in place to ensure that any risks are managed and to meet client requirements for the fulfillment of travel services and associated processes.

The services provided by ATPI are subject to various security and privacy legislations including but not limited to GDPR, UK DP and those from the multiple global locations in which or for which ATPI 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 offered online. Security commitments are standardized and include, but are not limited to, the following:

Security principles within the fundamental designs of the propriety systems developed by ATPI that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

Use of encryption technologies to protect customer data both at rest and in transit.

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

Components of the System

Infrastructure

Primary infrastructure used to provide ATPI's Travel Management Services Booking System which includes booking travel to invoicing and reporting system includes the following:

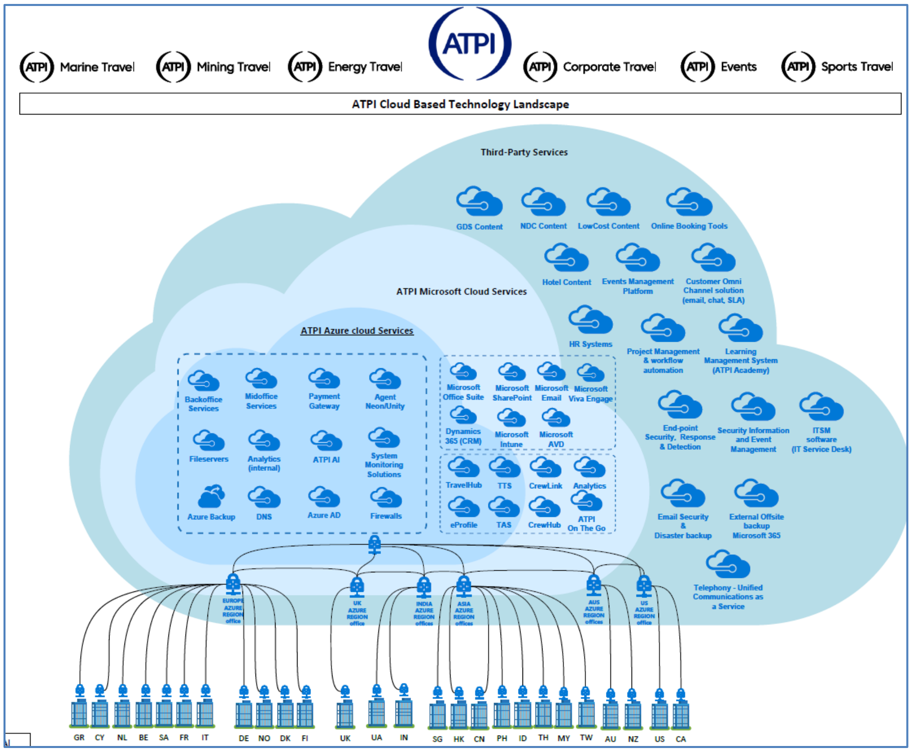
Primary Infrastructure		
Hardware	**Type**	**Purpose**
Cloud Provider	Azure	Cloud infrastructure and data storage
Switches	Various	Connects devices on the corporate network by sending messages to the specific device(s) that need to receive it
Servers/VM's	Various	Runs specific software on Windows or Linux operating system to support specific needs for the organization

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Laptops/Desktops	Various	Allows end-users to use various specific services within the organization while performing their daily tasks
Printer	Various	Facilitate printer services
Access Points	Ubiquity	Facilitates Wi-Fi access within the offices

Software

Primary software used to provide ATPI's Travel Management Services Booking System which includes booking travel to invoicing and reporting system includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Firewalls	FortiGate	Filters traffic into and out of the private network supporting the company services
IDS	Fortinet	Intrusion detection and alerting
Log Management	Rapid7	Monitoring and Logging Services
Vulnerability Management	Rapid7	Vulnerability Scanning Services



People

ATPI has a global staff headcount of approximately 2400. These staff are split across 26 countries and in various functions including:

- Operations: The largest department within the company including consultants, team leaders and management. These individuals use various tools to provide quotes and make bookings for travel services. Operations are split into different groups related to the types of clients they service including: Corporate Travel; Marine Travel; Energy Travel; Sports Travel; Yacht Travel; Mining Travel; Ancillary services (E.g. Visa) and Events.
- Sales & Account Management: These teams complete the RFPs and provide associated support to win new clients and drive revenue. Account Management maintain a high-level relationship with clients to ensure their continued satisfaction.
- Accounts / Finance: Supporting the client by ensuring the information from Operations is quality checked for completeness and providing the clients with invoices and statements relevant to the services they have in place. Supporting ATPI as a whole by managing and monitoring the budgets and spending of all departments within the company.
- Support Functions include Digital, MI, Marketing, HR, Compliance and Legal providing the support and advice that different teams need to provide a clear service.
- IT: This unit serves as the backbone of ATPI’s global IT environment, ensuring that systems, infrastructure, and support processes run smoothly to enable business continuity and productivity. The department’s primary objective is to maintain a stable and secure IT environment, provide exceptional end-user support, and continuously enhance operational processes to meet evolving business needs and technology advancements. Areas covered by IT are; Service Desk & End User Support, Desktop Delivery, Infrastructure & Cloud Management, Assets Management, Identity & Access Management (IAM) and Communication & Collaboration tools.
- Security Operations: Sec Ops continually analyze and mitigate the risks proactively: safeguarding the confidentiality, integrity and availability of the company’s informational assets.

Data

Data related to travelers along with their personal data like Title, Gender, First name, Last name and Middle name, Phone number, relatives’ phone numbers, E-mail address, Home address, Nationality, DOB, Passport information, Visa information, Seamans Document information, Rank, Grade as well as any other personal data required for the fulfilment of travel.

Processes, Policies and Procedures

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

Physical Security

ATPI uses Azure for cloud hosting services. Therefore, Azure is responsible for physical and environmental security of the hosted environments. Refer to the ‘Subservice Organizations’ section below for controls managed by Azure.

Logical Access

Access to ATPI's systems follows the principle of least privilege (PoLP) and is granted based on role-based access control (RBAC). Strong authentication mechanisms, including multi-factor authentication (MFA), are implemented where applicable to enhance security. Access requests, modifications, and removals undergo formal approval processes, with regular reviews conducted to ensure access remains appropriate. All access activities are logged and monitored to detect and respond to unauthorized attempts, ensuring the integrity and confidentiality of ATPI's systems and data.

Computer Operations - Backups

ATPI has established and enforces comprehensive policies governing Backups requirements. ATPI uses Azure Backup as the primary backup mechanism with both options LRS - Locally Redundant Storage (LRS) & GRS - Geo-Redundant Storage (GRS) in use depending on the system. With Azure Backup ATPI has a robust backup solution in place that is protecting ATPI's data in a secure (encrypted) way. There are different backup policies in place with retention policy set between 1 day up to 2 years depending on the system. For long term storage Azure BLOB storage technology is used. For some of the databases ATPI makes use of Azure Managed SQL solution offering the option Point in Time Restore (PITR). This means it is possible to select a point in time within the retention window (between 7 and 14 days) and restore the database to its previous state at that time (this can go back up to a day, an hour, a minute or a second).

For Office365 content (E-mail, OneDrive, Teams, SharePoint) in addition to Microsoft backup facility a backup-solution is utilized that allows the company to create an OFFSITE backup which provides a backup that does not depend on Microsoft's own backup.

Computer Operations - Availability

ATPI maintains a robust and resilient IT infrastructure to ensure high availability and operational continuity. The company's environment leverages a Virtual Desktop solution across six Azure regions utilizing Microsoft AVD, providing users with secure, scalable, and geographically distributed access to critical systems. Additionally, ATPI adopts a modern workspace strategy, prioritizing web-based access to core applications via Office 365 to enhance flexibility and operational efficiency. This dual approach enables seamless system availability while ensuring redundancy through cloud-based solutions. ATPI's policies and procedures include proactive capacity management, monitoring, patching and disaster recovery planning, ensuring minimal downtime and rapid recovery in case of incidents.

Change Control

ATPI has implemented a structured change management workflow to ensure that all modifications to systems, applications, and infrastructure are controlled, documented, and approved before execution. Change requests are managed via SharePoint, where they undergo a formal approval process by the CIO or designated IT Leads to assess potential risks and impacts. Additionally, ATPI utilizes a centralized helpdesk system across different supporting units to track and manage all support cases related to system changes. This structured approach ensures that changes are properly reviewed, implemented securely, and communicated effectively, maintaining system integrity and minimizing operational disruptions.

Specific For Discovery (mid-office system)

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system. Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers. When any system updates are implemented, key stakeholders are made aware at least seven days in advance unless an urgent patch release. The release process is also documented in advance and a checklist for release produced. This process is then followed by regression testing of the platform overall.

Data Communications

ATPI has established secure and resilient data communication processes to ensure the integrity, confidentiality, and availability of information across its network. The company's infrastructure leverages modern networking technologies and cloud-based solutions, ensuring secure communication between users, systems, and external partners. Data transmission is encrypted using industry-standard protocols to protect sensitive information. ATPI also enforces strict network access controls, monitoring, and firewall policies to prevent unauthorized access. Regular security assessments and monitoring are conducted to detect and mitigate potential threats, ensuring a secure and reliable data communication environment for business operations.

Penetration testing is performed using a CREST certified external organization; vulnerability scanning is done weekly. ATPI has internal, external and application vulnerability scanning.

New and emerging threats and vulnerabilities are monitored by the Group Information Security Officer and where necessary raised for action. The company monitors and scans NIST and CVE (vulnerabilities DB) for new and emerging vulnerabilities. All issues are logged and tracked to remediation by the Security Team, and overdue issues escalated to the Risk Committee where applicable.

ATPI have implemented vulnerability scanning (internal; external and application), regular penetration tests, automated patches, upgraded anti-malware, put in a new generation firewall, threat intelligence service, SIEM/SOC, DLP, phishing simulation, certified ISO27001/ISO27018 supported by SIEM/SOC and MDR service and more.

We have regular meetings with the board on the security status, emerging risks and threats to the business. The security dashboard in place tracks any changes in the security posture enabling monitoring and acting upon any change in behavior.

Boundaries of the System

The scope of this report includes the Travel Management Services Booking System which includes booking travel to invoicing and reporting system performed in all the ATPI offices globally. However, the HR aspect was only reviewed with regard to the four countries, namely Germany, Netherlands, United Arab Emirates - Dubai, United Kingdom, and remote facilities.

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

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

Control Environment

Integrity and Ethical Values

Integrity and ethical values are essential elements of ATPI's culture. This is evidenced within the various Global policies including (but not limited to):

- Anti-Harassment & Anti-Bullying Policy
- Group Equality, Diversity & Inclusivity Policy
- Corporate Social Responsibility
- Fraud Policy
- Anti-Bribery & Corruption Policy
- Corporate Social Governance

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.
- Contracted employees sign an acknowledgment as part of their employment contract 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 and forms part of the employment contract.
- Various ATPI training courses are also monitored for completeness to ensure all employees have awareness of the ATPI requirements for Integrity and Ethical values.
- Reference checks are performed for employees as a component of the hiring process.

Commitment to Competence

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

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

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

Management's Philosophy and Operating Style

ATPI's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to identifying 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 and Subject Matter Experts (e.g. IT) annually complete a risk assessment to identify and monitor any relevant risks.
- Management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

ATPI's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

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

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

- Documented job descriptions are in place to communicate key areas of authority and responsibility.

- Training paths are in place to communicate key areas of authority and responsibility.
- Documented job descriptions are communicated to employees and updated as needed.
- Training paths are communicated to employees and updated as needed.

Human Resource Policies and Practices

As a Global organization, ATPI has both Global and Local HR Policies and Procedures in order to meet the relevant legislation of the countries in which it operates.

Global policies are reviewed annually (or more often should there be a significant change) and shared on a SharePoint site for access by all staff. Local policies and procedures are periodically reviewed and shared on local HR tools which the local staff have access to. Where there is a discrepancy between Global and Local policies, the policy with the stronger stance is the one that is taken as superior.

All new employees are provided with contracts, which include confidentiality clauses for the protection of the company's staff and clients. Inductions and initial training is to be completed within one month of starting with the company and there are annual training requirements for all employees.

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

- Employee evaluations are carried out at a local level and these drive career progression and improvements.
- Onboarding and termination procedures for employees involve several departments to ensure the appropriate access and permissions are in place.

Risk Assessment Process

The Information Security Management System Risk Assessment procedure is based upon the mandatory requirements of ISO 27001:2022, to document the Information Security (IS) Risk Assessment (RA) process. The procedure establishes the methodology and frequency of RA for all offices (including UK, NL. GER, UAE) in scope of certification. Whilst the other offices are not within the scope of ISO 27001 they all follow the ISO 27001 framework.

The procedure is to ensure that the IS-Risk Assessment process is consistent in all locations, and fully conforms to the requirements of clause 6.1.2 of ISO 27001:2022 which are:

a) Establish & maintain IS risk criteria
b) Identifying IS risks
c) Analyzing IS risks
d) Evaluating IS risks

Further details of this procedure can be provided upon request.

In addition to the above procedure, there is also an Integrated Management System Risk Identification and Management Procedure. The core risk management process is as follows:

a) Ensuring that a process exists for communication between, and consultation, with internal and external stakeholders regarding the understanding, assessment and management of risk.
b) Describing the environment in which the company operates. This is described within the IMS as the 'Context' of the company. This will typically include the following:
    - Social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive factors, and the extent to which these differ at the international, national, regional and local levels
    - Key drivers and any trends that impact on the objectives of the company
    - Effect of the contractual and non-contractual relationships with, and the perceptions and values of, internal and external stakeholders

- Internal governance, organizational structure, roles and responsibilities, and the policies, objectives, and the strategies that are in place to support and achieve them
- Company's capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies, and its culture, decision making processes (both formal and informal), information flows & information systems

c) The system for defining Risk is based largely on meeting the needs and expectations of Interested Parties. This process includes the identification of those Parties, and understanding their needs & expectations, and any risks associated with not meeting those needs. Any risks arising will be raised within the company's risk register to be assessed and then eliminated (where possible), mitigated, or managed. The risk register will also contain risks that senior management identify within their monthly reports.

d) The Risk Assessment system, which includes risk identification, analysis and evaluation:

- The company will have appropriate risk identification tools and techniques that are suited to its objectives and capabilities, and to the risks faced, and people with the appropriate knowledge will be involved in identifying risks.
- Risk analysis involves developing an understanding of the risk and is analyzed by determining consequences and their likelihood, and other attributes of the risk. Clearly, a risk event can have multiple consequences and can affect multiple company management systems and objectives.

e) Risk treatment is the selection by the company of one or more solutions for reducing risks based on the widely understood 'Hierarchy of Risks' (especially for Health & Safety risks) although it can also introduce new risks including those arising from new opportunities. It is a cyclical process that aims to reduce the gross risk to an acceptable or target risk level by applying a risk treatment plan and then assessing the effectiveness of that plan. Examples of risk treatment options or controls are:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- Taking or increasing the risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood or the impact / consequences
- Sharing the risk with another party or parties (including insurance & joint contracts)
- Retaining the risk if it is believed it is understood and can be tolerated

f) Monitoring and Review of the process is necessary in order to improve it. In this way, the company will have confidence that controls are effective and efficient, lessons are learned from events, changes, trends and failures, that the process adapts to changes to the risk environment, and that emerging risks are identified.

g) Recording of the Risk Management Process. This is done using the company's Compliance GRC system for risk management, supplemented by periodic management reports and audits.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of ATPI's Travel Service which includes booking travel to the invoicing and reporting system; as well as the nature of the components of the system result in risks that the criteria will not be met. ATPI 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, ATPI's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

ATPI utilizes a secure and modern information and communication system to ensure efficient collaboration and data exchange across the organization. The infrastructure is built on a hybrid cloud model, leveraging Microsoft Office 365 for e-mail, document management, and collaboration tools, alongside Azure Virtual Desktop (AVD) for controlled and secure system access where required. Communication channels, including Microsoft Teams, SharePoint, and a centralized helpdesk system, facilitate seamless internal and external interactions. Data exchanged within these systems is encrypted and monitored to ensure confidentiality and compliance with security policies. ATPI enforces strict access controls and regular audits to maintain the integrity and availability of its communication systems while ensuring alignment with regulatory requirements.

ATPI operates a global e-Learning Academy utilizing an online training and development system to ensure all staff are constantly updated with changes to processes, and legislation as it affects their country or region. ATPI Academy includes courses on security awareness, PCI, data protection, GDPR and more. There are also policies and procedures in place relating to Remote Access, Removable Media, Mobile Device use and more.

SecOps have operating procedures which cover the following:

- Identifying critical information
- Analyzing threats
- Analyzing vulnerabilities
- Determining risks
- Planning mitigation control

All policies, relevant procedures, work instructions, and documentation will be held within the SharePoint system and communicated by way of a training requirement on a specific record or enabling the records to be visible to those staff that need to see them for awareness and knowledge.

All audit reports, management review minutes, and other top-level documents will also be communicated in the same way to all staff (as appropriate).

Individual departments such as IT, Sec Ops, HR, etc. all hold various periodic meetings and collaborative meetings as required to ensure all relevant staff are aware of the various controls required as part of ATPI's operations.

Monitoring Controls

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

On-Going Monitoring

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

Management’s close involvement in ATPI’s operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision to address 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 ATPI’s personnel.

ATPI also undergoes with annual ISO27001 audit. ATPI is certified under ISO27001:2022 and ISO 27018 framework.

All the defined controls under the framework are implemented and audited in internal and external audit for ISO27001.

Reporting Deficiencies

All Major/ Critical incidents are reported to the SecOps, Compliance, respective stakeholders and e-mails is circulated to all the team to notify the same. Regular progress is also shared till the issue is resolved.

Incidence are reported to secOps@atpi.com all support requests are routed to support@atpi.com.

SIEM tool is implemented to track and monitor all the alerts which are notified.

Changes to the System in the Last 3 Months

ATPI migrated from Virtual Desktop offering by Citrix (Citrix DaaS) to Azure Virtual Desktop solution. The migration was completed during December, 2024.

Incidents in the Last 3 Months

No significant incidents have occurred to the services provided to user entities in the 3 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common/Security and Availability criteria was applicable to the ATPI Travel Management Services Booking System which includes booking travel to invoicing and reporting system.

Subservice Organizations

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

Subservice Description of Services

ATPI relies upon Azure to provide cloud hosting services. As such, Azure is responsible for the physical and environment security controls for the in-scope system.

ATPI relies upon TripStax to provide SaaS and PaaS services. As such, TripStax is responsible for the change management controls for the in-scope production applications.

Complementary Subservice Organization Controls

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

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

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.
		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.
Availability	A1.2	Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
		Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.
		Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Customer data is automatically replicated within Azure to minimize isolated faults.
		Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
		Backup restoration procedures are defined, and backup data integrity checks are performed through standard restoration activities.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		Offsite backups are tracked and managed to maintain accuracy of the inventory information.
		Production data is encrypted on backup media.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.

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

Subservice Organization - TripStax		
Category	**Criteria**	**Control**
Common Criteria / Security	CC8.1	The ability to migrate/merge changes into the production environment is restricted to authorized and appropriate users.
		A code/peer review is systematically required prior to deploying the PR into the production environment.

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

- Holding periodic discussions with vendors and subservice organizations
- Reviewing attestation reports over services provided by vendors and subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

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

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

1. User entities are responsible for understanding and complying with their contractual obligations to ATPI.
2. User entities are responsible for notifying ATPI 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 ATPI 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 ATPI services.

6. User entities are responsible for providing ATPI with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying ATPI 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 and Availability Categories)
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.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

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 ATPI’s description of the system. Any applicable trust services criteria that are not addressed by control activities at ATPI are described within Section 4 and within the Subservice Organization section 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 ATPI was limited to the Trust Services Criteria, related criteria and control activities specified by the management of ATPI and did not encompass all aspects of ATPI’s operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

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

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

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

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

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, 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.	Inquired of the Compliance Manager regarding the onboarding process to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the hiring procedures to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			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.	Testing of the control activity disclosed that the employee handbook and code of conduct were not acknowledged upon hire for two of five employees sampled. Subsequent testing of the control activity through inspecting the employee handbook acknowledgements disclosed that personnel were required to acknowledge the employee handbook and code of conduct.
		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 disciplinary policies to determine that sanction policies, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the group reporting inappropriate behavior policies and procedures to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	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 maintains independence from those that operate the key controls implemented within the environment.	Inspected the organizational chart and the completed 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 notes to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.	Inspected the completed internal controls matrix and management review meeting minutes to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal 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**
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	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 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 compliance and audit activities.	Inspected the completed internal control matrix to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.
		Executive management maintains independence from those that operate the key controls implemented within the environment.	Inspected the organizational chart and the completed internal controls matrix to determine that executive management maintained independence from those that operate the key 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.
		Executive management reviews the organizational chart and makes updates to the organizational structure and lines of reporting, if necessary.	Inspected the organizational chart to determine that executive management reviewed the organizational chart and made updates to the organizational structure and lines of reporting, if necessary.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint 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 completed 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.
		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.

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 vendor risk assessment is performed which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment for a sample of vendors to determine that a vendor risk assessment was performed 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 completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	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.

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 vendor risk assessment is performed which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment for a sample of vendors to determine that a vendor risk assessment was performed which included reviewing the activities performed by third-parties.	No exceptions noted.
		Policies and procedures are in place that outline the competency and training requirements for personnel.	Inspected the competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the competency and training requirements for personnel.	No exceptions noted.
		The entity evaluates the competencies and experience of candidates prior to hiring.	Inspected the resume for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring.	No exceptions noted.
		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 job opening postings and e-mails 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.
		Executive management has created a training program for its employees.	Inspected the information security and awareness training program to determine that executive management created a training program for its employees.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Control Environment

CC1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The entity has implemented a mentor program to develop its personnel.	Inspected the effectiveness program PowerPoint deck to determine that the entity created a mentor program for its employees.	No exceptions noted.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inquired of the Compliance Manager regarding the onboarding process to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the hiring procedures to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			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.	Testing of the control activity disclosed that the employee handbook and code of conduct were not acknowledged upon hire for two of five employees sampled. Subsequent testing of the control activity through inspecting the employee handbook acknowledgements disclosed that personnel were required to acknowledge the employee handbook and code of conduct.
		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 disciplinary 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint 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.
		Policies and procedures are in place that outline the competency and training requirements for personnel.	Inspected the competency and training requirements policies and procedures to determine that policies and procedures were in place that outlined the competency and training requirements for personnel.	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 Chief Information Officer 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.
			Observed the input of information into the in-scope system to determine that edit checks were in place to prevent incomplete or incorrect data from being entered into the system.	No exceptions noted.
			Inspected the 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.

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 flow diagrams, process flowcharts, narratives and procedures manuals are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the network diagram and data flow diagram to determine that data flow diagrams, process flowcharts, narratives and procedures manuals were documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
		Data entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the file integrity monitoring (FIM) configurations, IDS 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 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inquired of the Compliance Manager regarding the onboarding process to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			Inspected the hiring procedures to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
			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.	Testing of the control activity disclosed that the employee handbook and code of conduct were not acknowledged upon hire for two of five employees sampled. Subsequent testing of the control activity through inspecting the employee handbook acknowledgements disclosed that personnel were required to acknowledge the employee handbook and code of conduct.
		Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.	Inspected the group reporting inappropriate behavior policies and procedures to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's SharePoint site.	Inspected the job description for a sample of job roles and the entity's SharePoint 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.
		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 to determine that the entity's policies and procedures, code of conduct and employee handbook were made available to personnel through the entity's intranet 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 intranet 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**
		Upon hire, personnel are required to complete information security awareness training.	Inspected the information security awareness training tracking tool for a sample of new hires to determine that upon hire, personnel were required to complete information security awareness training.	No exceptions noted.
		Current employees are required to complete information security awareness training annually.	Inspected the information security awareness training 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 minutes 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.
		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.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Information and Communication</th></tr>
<tr><th>CC2.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>The entity's objectives, including changes made to the objectives, are communicated to its personnel through quarterly company-wide meetings.</td><td>Inspected the townhall meeting minutes for a sample of quarters to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through quarterly company-wide meetings.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.</td><td>Inspected the completed internal control matrix to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.</td><td>Inspected the incident management 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.</td><td>No exceptions noted.</td></tr>
<tr><td>CC2.3</td><td>COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.</td><td>Employees, third-parties, and customers are directed on how to report unethical behavior in a confidential manner.</td><td>Inspected the group reporting inappropriate behavior policies and procedures to determine that employees, third-parties, and customers were directed on how to report unethical behavior in a confidential manner.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place and 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 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 third-party agreement for a sample of third-parties to determine that the entity's third-party agreement communicated the system commitments and requirements of third-parties.	No exceptions noted.
		The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third-parties.	Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated the terms, conditions and responsibilities of third-parties.	No exceptions noted.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Information and Communication</th></tr>
<tr><th>CC2.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.</td><td>Inspected the customer agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Executive management meets annually with operational management to discuss the results of assessments performed by third-parties.</td><td>Inspected the management review meeting minutes to determine that executive management met annually with operational management to discuss the results of assessments performed by third-parties.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td>Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.</td><td>Inspected the incident management 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.</td><td>No exceptions noted.</td></tr>
</table>

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 notes 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 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 specific, measurable, attainable, relevant and time-bound (SMART).	No exceptions noted.
		Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.	Inspected the risk 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 has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	Inspected the documented key performance indicators for operational and internal controls effectiveness to determine that executive management established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.	No exceptions noted.
		Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.	Inspected the completed internal control matrix to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit 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**
		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 entity's documented objectives and strategies and the documented key performance indicators for operational and internal controls effectiveness to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies.	No exceptions noted.
		Business plans and budgets align with the entity's strategies and objectives.	Inspected the entity's business plans, budget, and documented objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives.	No exceptions noted.
		Entity strategies, objectives and budgets are assessed on an annual basis.	Inspected the management review meeting minutes to determine that entity strategies, objectives and budgets were assessed on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures.	Inspected the completed internal controls matrix to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures.	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 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.
		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**
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inquired of the Head of Compliance regarding risk mitigation to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the risk assessment and management policies and procedures to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment 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.	Testing of the control activity disclosed that there were no internal controls that failed during the review period.
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 which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment for a sample of vendors to determine that a vendor risk assessment was performed which included reviewing the activities performed by third-parties.	No exceptions noted.

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

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

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the completed risk assessment 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.	Testing of the control activity disclosed that there were no internal controls that failed during the review period.
		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.

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 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.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the 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.
		On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.	Inspected the completed fraud assessment to determine that, on an annual basis, management identified and assessed the types of fraud that could impact their business and operations.	No exceptions noted.
		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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities.	Inspected the 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.
		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 notes 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 which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment for a sample of vendors to determine that a vendor risk assessment was performed which included reviewing the activities performed by third-parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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.
		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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Changes in 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.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Performance and conduct evaluations are performed for personnel on an annual basis.	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 notes 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 which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment for a sample of vendors to determine that a vendor risk assessment was performed 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 compliance and audit activities.	Inspected the completed internal control matrix to determine that responsible parties were defined and assigned to coordinate and monitor 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, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		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 completed internal controls matrix to determine that on an annual basis, management reviewed the controls implemented within the environment for compliance and operational effectiveness and identified potential control gaps and weaknesses.	No exceptions noted.

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 data backup restoration test is performed annually.	Inquired of the Chief Information Officer regarding restoration testing to determine that a data backup restoration test was performed annually.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed annually.	No exceptions noted.
		Internal and external vulnerability scans are performed weekly and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results for a sample of weeks and the supporting ticket for a sample of vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed weekly and remedial actions were taken where necessary.	No exceptions noted.
		A third-party performs a penetration testing to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing to identify and exploit vulnerabilities identified within the 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**
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
		Logical access reviews are performed monthly.	Inquired of the Chief Information Officer regarding user access reviews to determine that logical access reviews were performed monthly.	No exceptions noted.
			Inspected the completed access review for the in-scope systems for a sample of months to determine that logical access reviews were performed monthly.	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 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				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 notes 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 compliance and audit activities.	Inspected the completed internal control matrix to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inquired of the Head of Compliance regarding risk mitigation to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the risk assessment and management policies and procedures to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.

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 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.	Testing of the control activity disclosed that there were no internal controls that failed during the review period.
		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 minutes to determine that senior management assessed the results of the compliance, control and risk assessments performed on the 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**
		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 vulnerabilities identified from a vulnerability scan or penetration test 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 vulnerabilities identified from a vulnerability scan or penetration test 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 vulnerabilities identified from a vulnerability scan or penetration test 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 compliance meeting minutes 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 completed 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 notes 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 compliance and audit activities.	Inspected the completed internal control matrix to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.
		Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	Inquired of the Head of Compliance regarding risk mitigation to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the risk assessment and management policies and procedures to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the completed risk assessment 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.	Testing of the control activity disclosed that there were no internal controls that failed during the review period.
		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 vulnerabilities identified from a vulnerability scan or penetration test to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control 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 completed internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Management has documented the relevant controls in place for each key business or operational process.	Inspected the completed internal controls matrix to determine that management documented the relevant controls in place for each key business or operational process.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the completed internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity plan to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Organizational and information security policies and procedures are documented and made available to personnel through the entity's 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.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the completed internal controls matrix to determine that management incorporated a variety of controls into their environment that 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 completed 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 completed internal controls matrix to determine that management documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the management review meeting notes 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.
		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 compliance and audit activities.	Inspected the completed internal control matrix to determine that responsible parties were defined and assigned to coordinate and monitor compliance and audit activities.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the completed internal controls matrix to determine that performance of the internal controls implemented within the environment were assigned to appropriate process owners and operational personnel based on roles and responsibilities.	No exceptions noted.
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the completed internal controls matrix to determine that management incorporated a variety of controls into their environment that included manual, automated, preventive, detective, and corrective controls.	No exceptions noted.
		The organizational and information security policies and procedures detail the day-to-day activities to be performed by personnel.	Inspected the organizational and information security policies and procedures to determine that the organizational and information security policies and procedures detailed the day-to-day activities to be performed by personnel.	No exceptions noted.
		Management has implemented controls that are built into the organizational and information security policies and procedures.	Inspected the organizational and information security policies and procedures and the completed internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.	Inspected the completed internal controls matrix to determine that process owners and key management were assigned ownership to each key internal control implemented within the entity's environment.	No exceptions noted.
		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 completed 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				
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, access control policies and procedures and password management 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 Chief Information Officer 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, production servers, 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 Chief Information Officer 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 Chief Information Officer 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.	Observed a user login to the network to determine that network users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Inspected the network user listing and network password settings to determine that network users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The network is configured to enforce password requirements that include: • Password history • Maximum password age • Minimum 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 • Minimum password age • Password length • Complexity	No exceptions noted.
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout settings to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Network audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.

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 audit logs are maintained for review when needed.	Inquired of the Chief Information Officer regarding network audit logs to determine that network audit logs were maintained for review when needed.	No exceptions noted.
			Inspected an example network audit log extract to determine that network audit logs were maintained for review when needed.	No exceptions noted.
		Production server user access is restricted via role based security privileges defined within the access control system.	Inquired of the Chief Information Officer 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 servers user listing and access roles 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 Chief Information Officer regarding administrative access to determine that production server administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production servers administrator listing and access roles to determine that production servers administrative access was restricted to authorized personnel.	No exceptions noted.

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

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 logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the production servers audit logging configurations and an example production server audit log extract to determine that production server audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Production server audit logs are maintained for review when needed.	Inquired of the Chief Information Officer 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 Chief Information Officer 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.

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 databases user listing and access roles 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 Chief Information Officer regarding administrative access to determine that database administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production databases administrator listing and access roles 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.	Observed a user login to the production databases to determine that production database users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Inspected the production databases password configurations to determine that production databases 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 databases are configured to enforce password requirements that include: • Password history • Maximum password age • Minimum password age • Password length • Complexity	Inspected the production databases password configurations to determine that production databases were configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the production databases account lockout configurations to determine that database 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 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 system events.	No exceptions noted.
		Production database audit logs are maintained for review when needed.	Inquired of the Chief Information Officer 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				
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 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 Chief Information Officer 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 applications user listing and access roles to determine that production application user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Production application administrative access is restricted to authorized personnel.	Inquired of the Chief Information Officer regarding administrative access to determine that production application administrative access was restricted to authorized personnel.	No exceptions noted.
			Inspected the production applications administrator listing and access roles to determine that production application 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**
		Production application users are authenticated via individually-assigned user accounts and passwords.	Observed a user login to the production applications to determine that production application users were authenticated via individually-assigned user accounts and passwords.	No exceptions noted.
			Inspected the production applications 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 • Minimum password age • Password length • Complexity	Inspected the production applications password configurations to determine that applications were configured to enforce password requirements that included: • Password history • Maximum password age • Minimum password age • Password length • Complexity	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access 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 • Account lockout counter reset	Inspected the production applications account lockout configurations to determine that application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		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 Chief Information Officer 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 Chief Information Officer 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 Chief Information Officer 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.
		The entity's various networks are segmented to keep information and data isolated and restricted to authorized personnel.	Inspected the DMZ settings and the cloud environment to determine that the entity's various networks were segmented to keep information and data isolated and restricted to authorized personnel.	No exceptions noted.
		Data coming into the environment is secured and monitored through the use of firewalls and an IDS.	Inspected the IDS configurations, firewall rule sets and the network diagram to determine that data coming into the environment was secured and monitored through the use of firewalls and an IDS.	No exceptions noted.

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 demilitarized zone (DMZ) is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.
		Server certificate-based authentication is used as part of the 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 TLS encryption with a trusted certificate authority.	No exceptions noted.
		Logical access reviews are performed monthly.	Inquired of the Chief Information Officer regarding user access reviews to determine that logical access reviews were performed monthly.	No exceptions noted.
			Inspected the completed access review for the in-scope systems for a sample of months to determine that logical access reviews were performed monthly.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Compliance Manager 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 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 as a component of the termination process.	Inquired of the Compliance Manager 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 ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Chief Information Officer 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**
CC6.2	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, access control policies and procedures and password management 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 Chief Information Officer 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, production servers, database and application to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Logical access reviews are performed monthly.	Inquired of the Chief Information Officer regarding user access reviews to determine that logical access reviews were performed monthly.	No exceptions noted.
			Inspected the completed access review for the in-scope systems for a sample of months to determine that logical access reviews were performed monthly.	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 approved and granted to an employee as a component of the hiring process.	Inquired of the Compliance Manager 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 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 as a component of the termination process.	Inquired of the Compliance Manager 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 ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Chief Information Officer 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.

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 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.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the information security policies and procedures, access control policies and procedures and password management 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 Chief Information Officer 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, production servers, 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 Chief Information Officer 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.
		Production server user access is restricted via role based security privileges defined within the access control system.	Inquired of the Chief Information Officer 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 servers user listing and access roles 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 Chief Information Officer 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 production databases user listing and access roles to determine that production databases 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 user access is restricted via role-based security privileges defined within the access control system.	Inquired of the Chief Information Officer 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 applications 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 monthly.	Inquired of the Chief Information Officer regarding user access reviews to determine that logical access reviews were performed monthly.	No exceptions noted.
			Inspected the completed access review for the in-scope systems for a sample of months to determine that logical access reviews were performed monthly.	No exceptions noted.
		Logical access to systems is approved and granted to an employee as a component of the hiring process.	Inquired of the Compliance Manager regarding the hiring process to determine that logical access to systems was approved and granted to personnel as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the 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 as a component of the termination process.	Inquired of the Compliance Manager 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 ticket for a sample of terminated employees to determine that logical access to systems was revoked from personnel as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the Chief Information Officer 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.	This criterion is the responsibility of the subservice organizations. Refer to the "Subservice Organizations section above for controls managed by the subservice organizations.	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 retention policies and procedures and data classification 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.
		The entity purges data stored on cloud backups, per a defined schedule.	Inspected the backup schedule and configurations to determine that the entity purged data stored on cloud backups, per a defined schedule.	No exceptions noted.
		Data that is no longer required is disposed of and rendered unreadable to meet the entity's objectives.	Inquired of the Chief Information Officer regarding disposal of data to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	No exceptions noted.
			Inspected the data retention policies and procedures and data classification policies and procedures to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
			Inspected the destruction certificate for a sample of requests to dispose of data, purge a system, or physically destroy a system to determine that data that was no longer required was disposed of and rendered unreadable to meet the entity's objectives.	Testing of the control activity disclosed that there were no requests to dispose of data, purge a system, or physically destroy a system during the review period.
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 Chief Information Officer 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.
		A demilitarized zone (DMZ) is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.
		Server certificate-based authentication is used as part of the 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 TLS encryption with a trusted certificate authority.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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.
		VPN, 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, TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Observed the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Chief Information Officer regarding access to stored data 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**
			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 for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rule sets for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configurations and an example IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	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 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 configurations for a sample of workstations and servers 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 except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.

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.	Server certificate-based authentication is used as part of the 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 TLS encryption with a trusted certificate authority.	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.
		VPN, 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, TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.	Observed the authentication of a user to the VPN to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.
			Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account and password before establishing a VPN session.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access to stored data is restricted to authorized personnel.	Inquired of the Chief Information Officer 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 for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rule sets for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configurations and an example IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		The ability to restore backups is restricted to authorized personnel.	Inquired of Chief Information Officer regarding restoring backed up data to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of users with the ability to restore backups to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.
		Backup data is replicated daily.	Inspected the backup replication configurations and an example backup replication log to determine that backup media was replicated daily.	No exceptions noted.
		Backup media is stored in an encrypted format.	Inspected the encryption configurations for an example backup media to determine that backup media was stored in an encrypted format.	No exceptions noted.

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**
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Production data is replicated to a separate and isolated availability zone continuously to achieve geo-redundancy.	Inspected the backup replication configurations to determine that production data was replicated to a separate and isolated availability zone continuously to achieve geo-redundancy.	No exceptions noted.
		Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring tool configurations, the antivirus software dashboard console, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		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 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 configurations for a sample of workstations and servers 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 Chief Information Officer regarding the applications and software to determine that the ability to install applications and software on workstations was restricted to authorized personnel.	No exceptions noted.
			Inspected the denial notification to determine that a warning notification appeared when an employee attempted to download an application or software.	No exceptions noted.
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM software configurations to determine that FIM software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		The FIM software is configured to notify IT personnel via alert when a change to the production application code files is detected.	Inspected the FIM software configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via alert when a change to the production application code files was detected.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		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 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, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Internal and external vulnerability scans are performed weekly and remedial actions are taken where necessary.	Inspected the completed vulnerability scan results for a sample of weeks and the supporting ticket for a sample of vulnerabilities identified by the vulnerability scans to determine that internal and external vulnerability scans were performed weekly and remedial actions were taken where necessary.	No exceptions noted.
		A third-party performs a penetration testing to identify and exploit vulnerabilities identified within the environment.	Inspected the completed penetration test results to determine that a third-party performed a penetration testing to identify and exploit vulnerabilities identified within the environment.	No exceptions noted.
		A firewall is in place to filter unauthorized inbound network traffic from the internet.	Inspected the network diagram and firewall rule sets for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.

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 for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configurations and an example IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM software configurations to determine that FIM software 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 FIM software is configured to notify IT personnel via alert when a change to the production application code files is detected.	Inspected the FIM software configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via 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 and configuration management 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 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, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the network account lockout settings to determine that network account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		Network audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the network audit logging configurations and an example network audit log extract to determine that network audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production server audit logging configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	Inspected the production servers audit logging configurations and an example production server audit log extract to determine that production server audit logging configurations were in place that included: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events	No exceptions noted.
		Production server audit logs are maintained for review when needed.	Inquired of the Chief Information Officer 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Database account lockout settings are in place that include: • Account lockout duration • Account lockout threshold	Inspected the production databases account lockout configurations to determine that database 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 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 system events.	No exceptions noted.
		Production database audit logs are maintained for review when needed.	Inquired of the Chief Information Officer 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Production application account lockout settings are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset	Inspected the production applications account lockout configurations to determine that application account lockout configurations were in place that included: • Account lockout duration • Account lockout threshold • Account lockout counter reset	No exceptions noted.
		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 Chief Information Officer 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				
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 for a sample of production servers to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.	No exceptions noted.
		The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.	Inspected the network diagram and firewall rule sets for a sample of production servers to determine that the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and IDS configurations to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.	No exceptions noted.
		The IDS is configured to notify personnel upon intrusion detection.	Inspected the IDS configurations and an example IDS alert notification to determine that the IDS was configured to notify personnel upon intrusion detection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 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 configurations for a sample of workstations and servers 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 except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.

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
		FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM software configurations to determine that FIM software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via alert when a change to the production application code files is detected.	Inspected the FIM software configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via 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 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**
		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 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.
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the management review 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 organizations. Refer to the “Subservice Organizations section above for controls managed by the subservice organizations.	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 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 management 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 management policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inspected the supporting incident report for an example critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
		Identified incidents are reviewed, monitored and investigated by an incident response team.	Inspected the supporting incident ticket for a sample of 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 an example critical security incident that resulted in unauthorized disclosure of personal information to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and communicated to the affected users.	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**
CC7.4	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 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.
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the management review 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 management 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 management policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Resolution of incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of incidents to determine that resolution of incidents were documented within the ticket and communicated to affected users.	No exceptions noted.
		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.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inspected the supporting incident report for an example critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
		The 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 management 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.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">System Operations</th></tr>
<tr><th>CC7.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>Critical security incidents that result in a service/business operation disruption are communicated to those affected through creation of an incident ticket.</td><td>Inquired of the Compliance Manager regarding incident management 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.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the incident management policies and procedures to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through creation of an incident ticket.</td><td>No exceptions noted.</td></tr>
<tr><td></td><td></td><td></td><td>Inspected the supporting incident ticket for an example critical security incident that resulted in a service/business operation disruption to determine that critical security incidents that result in a service/business operation disruption were communicated to those affected through creation of an incident ticket.</td><td>Testing of the control activity disclosed that there were no incidents that resulted in a service/business operation disruption during the review period.</td></tr>
<tr><td></td><td></td><td>Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.</td><td>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.</td><td>No exceptions noted.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The risks associated with identified vulnerabilities are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the supporting incident ticket for a 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 annually.	Inquired of the Chief Information Officer regarding restoration testing to determine that a data backup restoration test was performed annually.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed annually.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity plan to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed disaster recovery test results to determine that the business continuity and disaster recovery plans were tested 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**
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the management review 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 report for an example critical security incident to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	No exceptions noted.
		Change management requests are opened for incidents that require permanent fixes.	Inquired of the Chief Information Officer regarding incident management to determine that change management requests were required to be opened for incidents that required permanent fixes.	No exceptions noted.
			Inspected the change management policies and procedures to determine that change management requests were required to be opened for incidents that required permanent fixes.	No exceptions noted.

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 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.	Testing of the control activity disclosed that there were no incidents that required permanent fixes during the review period.
		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 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.
		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 plan 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.

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 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 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.	FIM software is utilized to help detect unauthorized changes within the production environment.	Inspected the FIM software configurations to determine that FIM software was utilized to help detect unauthorized changes within the production environment.	No exceptions noted.
		The FIM software is configured to notify IT personnel via alert when a change to the production application code files is detected.	Inspected the FIM software configurations and an example alert generated from the FIM software to determine that the FIM software was configured to notify IT personnel via alert when a change to the production application code files was detected.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in the change management process.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in the change management process.	No exceptions noted.
		The change management process has defined the following roles and assignments: • Authorization of change requests - Change Control Board • Impact Analysis - Project Lead • Implementation - Project manager or Change Control Board	Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests - Change Control Board • Impact Analysis - Project Lead • Implementation - Project manager or Change Control Board	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 communicated to both affected internal and external users.	Inspected the newsletter to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
		System changes are authorized and approved by management prior to implementation.	Inspected the supporting change ticket for a sample of system changes to determine that system changes were authorized and approved by management prior to implementation.	No exceptions noted.
		Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.	Inspected the change control software 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.
		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 system 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.
		System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected the supporting change ticket for a sample of system changes to determine that system changes were tested prior to implementation, and that types of testing performed depended on the nature of the change.	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.

<table>
<tr><th colspan="5">TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY</th></tr>
<tr><th colspan="5">Change Management</th></tr>
<tr><th>CC8.0</th><th>Criteria</th><th>Control Activity Specified by the Service Organization</th><th>Test Applied by the Service Auditor</th><th>Test Results</th></tr>
<tr><td></td><td></td><td>Part of this criterion is the responsibility of the subservice organizations. Refer to the “Subservice Organizations section above for controls managed by the subservice organizations.</td><td>Not applicable.</td><td>Not applicable.</td></tr>
</table>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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.	Inquired of the Head of Compliance regarding risk mitigation to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.
			Inspected the risk assessment and management policies and procedures to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the completed risk assessment 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.	Testing of the control activity disclosed that there were no internal controls that failed during the review period.
		Documented policies and procedures are in place to guide personnel in performing risk assessment and risk mitigation activities.	Inspected the risk assessment and management policies and procedures to determine that documented policies and procedures were in place to guide personnel in performing risk assessment and risk mitigation activities.	No exceptions noted.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.
		Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the vendor management policies and procedures to determine that identified third-party risks were rated using a risk evaluation process and ratings 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**
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	A vendor risk assessment is performed which includes reviewing the activities performed by third-parties.	Inspected the vendor risk assessment policies and procedures and completed vendor risk assessment for a sample of vendors to determine that a vendor risk assessment was performed 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.
		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**
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports or vendor questionnaire for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.
		Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.	Inspected the vendor management policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the vendor management policies and procedures 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 management policies and procedures to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		The entity's third-party agreement outlines and communicates: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	Inspected the third-party agreement for a sample of third-parties to determine that the entity's third-party agreement outlined and communicated: • The scope of services • Roles and responsibilities • Terms of the business relationship • Communication protocols • Compliance requirements • Service levels • Just cause for terminating the relationship	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		A formal third-party risk assessment is performed 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 to identify threats that could impair system commitments and requirements.	No exceptions noted.
		Management has established exception handling procedures for services provided by third-parties.	Inspected the 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 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.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its 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, FIM configurations, IDS configurations, and firewall rule sets to determine that monitoring software was used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	No exceptions noted.
		The monitoring software is configured to alert IT personnel when thresholds have been exceeded.	Inspected the monitoring tool configurations, an example alert generated from the FIM software and an example IDS alert notification to determine that the monitoring software was configured to alert IT personnel when thresholds were exceeded.	No exceptions noted.
		Processing capacity is monitored 24x7x365.	Inspected the monitoring tool configurations to determine that processing capacity was monitored 24x7x365.	No exceptions noted.
		Future processing demand is forecasted and compared to scheduled capacity on a bi-weekly basis.	Inspected the annual future processing capacity demand forecast to determine that future processing demand was forecasted and compared to scheduled capacity on a bi-weekly basis.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	The ability to restore backups is restricted to authorized personnel.	Inquired of Chief Information Officer regarding restoring backed up data to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of users with the ability to restore backups to determine that the ability to restore backups was restricted to authorized personnel.	No exceptions noted.
		Backup data is replicated daily.	Inspected the backup replication configurations and an example backup replication log to determine that backup media was replicated daily.	No exceptions noted.
		Full backups of certain application and database components are performed on a daily basis.	Inspected the backup configurations and a backup log for a sample of days to determine that full backups of certain application and database components were performed on a daily basis.	No exceptions noted.
		When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure.	Inspected the backup configurations and the backup alert for a sample of failed backups to determine that when a backup job failed, the backup tool sent an alert to the backup administrators who investigated and resolved the failure.	No exceptions noted.
		Production data is replicated to a separate and isolated availability zone continuously to achieve geo-redundancy.	Inspected the backup replication configurations to determine that production data was replicated to a separate and isolated availability zone continuously to achieve geo-redundancy.	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Redundant architecture is in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	Inspected the business continuity plan and network diagram to determine that redundant architecture was in place to migrate business operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	No exceptions noted.
		A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.	Inspected the business continuity plan to determine that a business continuity plan was documented and in place that outlined the range of disaster scenarios and steps the business would take in a disaster to ensure the timely resumption of critical business operations.	No exceptions noted.
		The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	Inspected the completed disaster recovery test results to determine that the business continuity plan was tested on an annual basis and included: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	No exceptions noted.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	**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 organizations. Refer to the “Subservice Organizations section above for controls managed by the subservice organizations.	Not applicable.	Not applicable.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A data backup restoration test is performed annually.	Inquired of the Chief Information Officer regarding restoration testing to determine that a data backup restoration test was performed annually.	No exceptions noted.
			Inspected the completed backup restoration test to determine that a data backup restoration test was performed annually.	No exceptions noted.
		Business continuity and disaster recovery plans are developed and updated on an annual basis.	Inspected the business continuity plan to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		A business continuity 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 plan 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.

ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY				
A1.0	Criteria	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.	Inspected the business continuity plan to determine that a business continuity plan was documented and in place that outlined the range of disaster scenarios and steps the business would take in a disaster to ensure the timely resumption of critical business operations.	No exceptions noted.
		The business continuity plan is tested on an annual basis and includes: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	Inspected the completed disaster recovery test results to determine that the business continuity plan was tested on an annual basis and included: • Various testing scenarios based on threat likelihood • Identifying the critical systems required for business operations • Assigning roles and responsibilities in the event of a disaster • Assessing and mitigating risks identified as a result of the test disaster	No exceptions noted.

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	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.	Testing of the control activity disclosed that the employee handbook and code of conduct were not acknowledged upon hire for two of five employees sampled. Subsequent testing of the control activity through inspecting the employee handbook acknowledgements disclosed that personnel were required to acknowledge the employee handbook and code of conduct.	In the new UK HR system as part of the onboarding process, there will be a document guiding new starters to the Company Handbook / People policies and they will need to check a box to acknowledge that they have read and understood the documents. We are currently having our training on the Safeguarding sessions of People Hub so we would anticipate by September that these documents will all be uploaded to People Hub ready for when new starters commence employment with us. However, all the sampled employees have acknowledged the company policy - Acceptable Usage Policy, for which the evidence was shared during the audit.