A-LIGN

Astute Business Solutions

Type 2 SOC 2

2024

ASTUTE BUSINESS SOLUTIONS

REPORT ON ASTUTE BUSINESS SOLUTIONS' DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY

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

November 1, 2023 to October 31, 2024

Table of Contents

SECTION 1 ASSERTION OF ASTUTE BUSINESS SOLUTIONS MANAGEMENT 1

SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT 3

SECTION 3 ASTUTE BUSINESS SOLUTIONS' DESCRIPTION OF ITS MANAGED CLOUD SERVICES SYSTEM THROUGHOUT THE PERIOD NOVEMBER 1, 2023 TO OCTOBER 31, 2024 7

OVERVIEW OF OPERATIONS 8
Company Background 8
Description of Services Provided 8
Principal Service Commitments and System Requirements 9
Components of the System 9
Boundaries of the System 13
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING 13
Control Environment 13
Risk Assessment Process 15
Information and Communications Systems 15
Monitoring Controls 16
Changes to the System Since the Last Review 16
Incidents Since the Last Review 16
Criteria Not Applicable to the System 16
Subservice Organizations 16
COMPLEMENTARY USER ENTITY CONTROLS 18
TRUST SERVICES CATEGORIES 19

SECTION 4 TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS 20

GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS 21
CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION 22
TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY 22

SECTION 1

ASSERTION OF ASTUTE BUSINESS SOLUTIONS MANAGEMENT

ASSERTION OF ASTUTE BUSINESS SOLUTIONS MANAGEMENT

November 14, 2024

We have prepared the accompanying description of Astute Business Solutions' ('Astute' or 'the Company') Managed Cloud Services System titled "Astute Business Solutions' Description of Its Managed Cloud Services System throughout the period November 1, 2023 to October 31, 2024" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Managed Cloud Services System that may be useful when assessing the risks arising from interactions with Astute's system, particularly information about system controls that Astute has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Astute uses Amazon Web Services, Inc. ('AWS') to provide virtual desktop infrastructure (VDI) services and Oracle Cloud Infrastructure ('OCI') to provide cloud hosting 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 Astute, to achieve Astute's service commitments and system requirements based on the applicable trust services criteria. The description presents Astute's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Astute'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 Astute, to achieve Astute's service commitments and system requirements based on the applicable trust services criteria. The description presents Astute's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Astute's controls.

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

a. the description presents Astute's Managed Cloud Services System that was designed and implemented throughout the period November 1, 2023 to October 31, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Astute'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 Astute's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Astute'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 Astute's controls operated effectively throughout that period.

Arvind Rajan
Chief Executive Officer
Astute Business Solutions

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Astute Business Solutions

Scope

We have examined Astute's accompanying description of its Managed Cloud Services System titled "Astute Business Solutions' Description of Its Managed Cloud Services System throughout the period November 1, 2023 to October 31, 2024" (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 November 1, 2023 to October 31, 2024, to provide reasonable assurance that Astute's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Astute uses AWS to provide VDI services and OCI to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Astute, to achieve Astute's service commitments and system requirements based on the applicable trust services criteria. The description presents Astute's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Astute'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 Astute, to achieve Astute's service commitments and system requirements based on the applicable trust services criteria. The description presents Astute's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Astute's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Astute 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 Astute's service commitments and system requirements were achieved. Astute has provided the accompanying assertion titled "Assertion of Astute Business Solutions Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Astute 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,

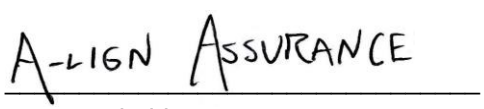
a. the description presents Astute's Managed Cloud Services System that was designed and implemented throughout the period November 1, 2023 to October 31, 2024, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Astute'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 Astute's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Astute'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 Astute'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 Astute, user entities of Astute's Managed Cloud Services System during some or all of the period November 1, 2023 to October 31, 2024, business partners of Astute subject to risks arising from interactions with the Managed Cloud Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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



Tampa, Florida
November 14, 2024

SECTION 3

ASTUTE BUSINESS SOLUTIONS' DESCRIPTION OF ITS MANAGED CLOUD SERVICES SYSTEM THROUGHOUT THE PERIOD NOVEMBER 1, 2023 TO OCTOBER 31, 2024

OVERVIEW OF OPERATIONS

Company Background

Astute was founded in 2006 by two PeopleSoft employees hoping to create an independent consulting firm, Astute is a provider of functional and technical consulting services and solutions beginning with PeopleSoft, and growing to include other technologies including Oracle Cloud, and managed cloud hosting services for PeopleSoft, Ellucian Banner, Oracle Business Suite, and related cloud workloads and management.

Astute helps its clients transform their organizations with cloud infrastructure and managed services to reduce total cost of ownership (TCO), improve performance, enhance security, and maximize return on investment.

Astute is a member of the Modern Oracle Partner Network as an Oracle Partner certified to sell, implement, and manage technologies on Oracle Cloud with specialization as a Cloud Service Provider (CSP).

In the last 17 years Astute has done work in almost every sector. Currently Astute's focus is on Higher Education, State and Local Government, Financial Services, Healthcare, and Manufacturing.

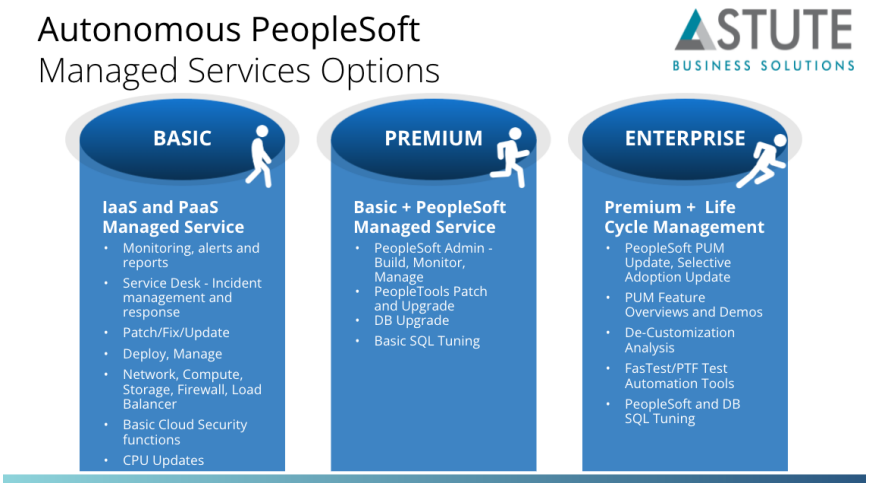
Description of Services Provided

Advisory Services - Astute is a full-service consultancy firm, capable of engaging to provide assessment work, thought leadership, feasibility studies, proof-of-concept, pre-planning, business case development, or any type of ad-hoc consulting a client may require on many of topics related to Oracle Technologies, PeopleSoft, Banner, and cloud migration.

Project-Based Services - Often resulting as a direct referral from an Oracle Sales Representative, or from word of mouth in user communities, project services include but are not limited to: PeopleSoft Projects (upgrades, modernization, updates, patches, module implementations, PTF implementation, cloud migrations), Banner Projects (upgrades, modernization, module implementation, cloud migration), Oracle Analytics Cloud (implementation).

Managed Services - Custom Service packages created for PeopleSoft or Banner Customers who are looking to offload management of part or the entirety of their system. Managed services could be sold a-la-carte such as a patching service, disaster recovery, or a tuning service, or might include a whole genre of services such as Infrastructure Services, Database Services, and / or Application services.

Astute uses this slide to describe managed services at a high level to prospective customers:



Principal Service Commitments and System Requirements

The principal service commitments for each customer will vary depending on the services provided. The details are covered in each contract's Statement of Work (SOW). The SOW outlines what is expected of the Company and the Customer, who has responsibility and accountability for what, and how the teams will get the work done.

Astute's primary business is as a technology services partner specializing in managed services on-premises and in the cloud for security, network, storage, compute, database, and application management for Oracle applications (PeopleSoft, E-Business Suite, JD Edwards, Hyperion, OBIEE, Oracle Analytics Cloud, Custom Applications on the Oracle DB) as well as Ellucian Banner.

At present Astute has several migration projects going. Some of those are for financial services companies. Some are for higher education.

Astute also has several managed services contracts in place, those cover higher education, not-for-profit, manufacturing logistics, and financial services.

Astute bases its services on the ITIL framework and looks to ISO and NIST for guidance on its security standards.

Components of the System

Infrastructure

Primary infrastructure used to provide Astute's Managed Cloud Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
OCI Virtual Cloud Network	Networking	Virtualized networking
OCI Storage	Storage	Virtualized storage
OCI Compute	Compute	Virtualized servers
Oracle Cloud Platform	Database	Database as a Service
Amazon WorkSpaces	VDI	Virtual desktop infrastructure ('VDI') services
Windows Laptops	Physical Desktop	Desktop Environment for Employees
Chromebook	Physical Desktop	Desktop Environment for Employees

Software

Primary software used to provide Astute's Managed Cloud Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Oracle CloudGuard	Cloud Based	Monitoring for suspicious activity
Oracle Log Analytics Service	Cloud Based	Aggregating, indexing, and analyzing logged data for various technology layers

Primary Software		
Software	**Operating System**	**Purpose**
Oracle Information Technology (IT) Analytics Service	Cloud Based	Monitoring performance, availability, and capacity of supporting infrastructure
Oracle Enterprise Manager Cloud Control	Cloud Based	Cloud lifecycle management system

People

Astute has 60 employees / contractors based in the US, Canada, and India organized in the following areas:

- Executive
- Finance / Accounting
- Human Resources
- Sales / Marketing
- Information Security and Information Systems
- Technical Service Delivery
- Business Service Delivery
- Project Management Office

As Astute is small, the Executive / Managerial roles are filled by many of the same people wearing different hats. Most of the staff / consultants reside in the Technical Delivery / Service Delivery teams. The common job descriptions on these teams are Application Administrator, Database Administrator, Functional Consultant, Network Administrator, Architect, etc.

The Chief Executive Officer (CEO), Chief Financial Officer (CFO), and Chief Technology Officer (CTO) are responsible for Sales / Marketing in addition to their other responsibilities.

The CFO also acts as the Chief Human Resources Officer (CHRO).

The CTO also acts as the Chief Information Security Officer (CISO).

Data

Data processed by the systems depends on the customer. In general, PeopleSoft and Banner are both ERP (enterprise resource planning) systems. These systems are tightly integrated systems that manage many different business processes for an organization. PeopleSoft addresses the different types of audiences as “pillars.”

PeopleSoft Pillars:

- Human Capital Management
- Finance / Supply Chain
- Enterprise Learning Management
- Customer Relationship Management
- Student
- Portal

Each of the PeopleSoft pillars may have two or more handfuls of modules including, but not limited to for example: Accounts Payable (AP), Account Receivable (AR), General Ledger (GL), Fixed-Assets.

Banner is similar but earns its heritage as a Student Information System.

As a managed service provider, Astute does not assume full responsibility for the customer's data. Astute acts as secure steward of customer data by managing customer systems on their behalf either on premises or on the Oracle Cloud, ownership of the data remains with the customer.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to Astute's policies and procedures that define how services should be delivered. These are located on the entity's intranet and can be accessed by any Astute team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by Amazon Web Services, Inc. (AWS) and Oracle Cloud Infrastructure (OCI). As such, AWS and OCI are responsible for the physical security controls for the in-scope system. Refer to the 'Subservice Organizations' section below for controls managed by AWS and OCI.

Logical Access

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

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

Employees authenticate to the Amazon WorkSpaces secure environment using an Active Directory user ID, password, and Duo factor authentication (MFA). Users are required to have membership to a unique Active Directory group in order to access the Amazon WorkSpaces secure environment. Passwords must conform to defined password standards and are enforced through parameter settings in the Active Directory. These settings are part of the configuration standards and force users to create complex passwords with a specified minimum password length, disable the user ID's ability to access the system and components after a specific specified number of unsuccessful access attempts and lockout workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Upon hire, employees are assigned to a position by human resources. Prior to the employees' start date, an onboarding request is created by human resources in Asana for the IT team. IT creates a checklist of accounts and permission levels needed for that role. The owner of each resource reviews and approves account creation and the associated permissions. IT, then works with the owner of each resource to set up the user.

Astute utilizes strong passwords that must be changed every 90 days and requires MFA for access to systems.

When an employee is terminated, the termination request is entered into the human resources system workflow by a member from the human resources team, and the security team will de-provision the employee's accounts.

On a monthly basis management reviews user access to the in-scope systems. Role lists are generated by the CTO and distributed to the appropriate reviews via the event management system. The reviewer inspects the access listings and indicates the required changes within the event ticket. Access changes are reported using the access administration process.

Computer Operations - Backups

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

Backups for customer systems are defined at the time they are onboarded and are validated as part of the pre-go live checklist.

Computer Operations - Availability

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

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

- Disk storage
- Network bandwidth

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

Change Control

As a managed service provider, Astute is not developing its own software. Astute does, however, deploy software on behalf of its customers, and in some cases, may have developers who develop software on a customer's behalf as requested by the customer. Astute follows standard SDLC processes and does have a defined change control policy and procedure that defines how change is implemented from environment to environment and how configuration changes are tracked.

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 when needed. Development and testing are performed in an environment that is logically separated from the production environment. Management and the customer approve changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control is maintained manually to maintain source code versions and migrate source code through the development process to the production environment. Version control is stored within Google Drive to maintains a history of code changes to support rollback capabilities and tracks changes to developers.

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

Data Communications

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

Redundancy is built into the OCI to help ensure that there is no single point of failure that includes firewalls, routers, and servers. If a primary system fails, the redundant hardware is configured to take its place.

Vulnerability scanning is performed by operation personnel on a monthly basis in accordance with Astute policy. Astute users Oracle Cloud Guard for vulnerability scanning and a formal methodology specified by Astute. Oracle Cloud Guard is used to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Astute system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Customer environments are only accessed via secure AWS workspace bastions. Access is authenticated through the use of MFA.

Penetration testing can be conducted on customer managed environments at the customer's discretion to measure the security posture of a target system or environment.

Boundaries of the System

The scope of this report includes the Managed Cloud Services System performed by Astute resources in Dublin, California.

This report does not include the VDI services provided by AWS, or the cloud hosting services provided by OCI at multiple facilities.

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

Control Environment

Integrity and Ethical Values

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

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

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook
- Background checks are performed for employees as a component of the hiring process

Commitment to Competence

Astute'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 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 jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

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

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

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

Organizational Structure and Assignment of Authority and Responsibility

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

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

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

Human Resource Policies and Practices

Astute's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Astute's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

Astute's risk assessment process identifies and manages risks that could potentially affect Astute's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Astute identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Astute's Managed Cloud Services System; as well as the nature of the components of the system result in risks that the criteria will not be met. Astute 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, Astute'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

Astute currently holds the following meetings for communication:

- Daily Project Meetings
- Daily Technical All-Hands Meetings
- Weekly Sales Forecast Meetings
- Semi-Monthly Resource Planning Meetings
- Monthly Marketing Meetings
- Quarterly All-Company Meetings

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

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

Specific information systems used to support Astute's Managed Cloud Services System are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Astute's management performs monitoring activities to 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

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

Reporting Deficiencies

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

Changes to the System Since the Last Review

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

Incidents Since the Last Review

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

Criteria Not Applicable to the System

All Common/Security criterion was applicable to the Astute's Managed Cloud Services System.

Subservice Organizations

This report does not include the VDI services provided by AWS, or the cloud hosting services provided by OCI at multiple facilities.

Subservice Description of Services

AWS provides VDI services for Astute's employees, and OCI provides cloud hosting services for Astute's customers, which include implemented physical security controls to protect the data managed by the in-scope service. Refer to the Complementary Subservice Organization Controls section below for controls managed by the subservice organizations.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Trust Services Criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Security	CC6.4, CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

The following subservice organization controls should be implemented by OCI to provide additional assurance that the Trust Services Criteria described within this report are met:

Subservice Organization - OCI		
Category	**Criteria**	**Control**
Security	CC6.4, CC7.2	Data center server floors network rooms and security systems are physically isolated from public spaces and / or delivery areas.
		Access to sensitive data center zones requires approval form authorized personnel and is controlled via badge access readers, biometric identification mechanism, and / or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.

Subservice Organization - OCI		
Category	**Criteria**	**Control**
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.

Astute management, along with the subservice organizations, 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, Astute performs monitoring of the subservice organization controls, including reviewing attestation reports over services provided by vendors and the subservice organizations.

COMPLEMENTARY USER ENTITY CONTROLS

Astute'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 Astute's services to be solely achieved by Astute control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Astute'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 Astute.
2. User entities are responsible for notifying Astute of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Astute 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 Astute services.
6. User entities are responsible for providing Astute with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Astute of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
8. User entities are responsible for managing operating system, database and application access to their own systems of record.
9. User entities are responsible for managing authentication settings for operating system, database and application access to their own systems of record.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

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

Control Activities Specified by the Service Organization

The applicable Trust Services Criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable Trust Services Criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Astute's description of the system. Any applicable Trust Services Criteria that are not addressed by control activities at Astute are described within Section 4 and within the 'Subservice Organizations' 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 Astute was limited to the Trust Services Criteria, related criteria and control activities specified by the management of Astute and did not encompass all aspects of Astute's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

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

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

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

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

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.	Inspected the employee handbook and code of conduct, the written information security program and the entity's intranet to determine that core values were communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.	No exceptions noted.
		An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.	Inspected the employee handbook and the code of conduct to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.	No exceptions noted.
		Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Prior to employment, personnel are required to complete a background check.	Inspected the background check policy and procedure and the completed background check for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance appraisals policy and the completed performance and conduct evaluation 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 policy to determine that sanction policies, which include probation, suspension and termination, were in place for employee misconduct.	No exceptions noted.
		An anonymous channel is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Inspected the whistleblower reporting site and the anonymous reporting form to determine that an anonymous channel was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior.	Inspected the whistleblower reporting site and the anonymous reporting form to determine that employees, third-parties, and customers were directed on how to report unethical behavior.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Upon hire, personnel are required to sign a confidentiality agreement.	Inspected the signed confidentiality agreement for a sample of new hires to determine that upon hire, personnel were required to sign a confidentiality agreement.	No exceptions noted.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Executive management roles and responsibilities are documented and reviewed annually.	Inspected the executive management job descriptions for a sample of executive roles to determine that executive management roles and responsibilities were documented and reviewed annually.	No exceptions noted.
		Executive management defines and documents the skills and expertise needed among its members.	Inspected the executive management job descriptions to determine that executive management defined and documented the skills and expertise needed among its members.	No exceptions noted.
		Executive management evaluates the skills and expertise of its members annually.	Inspected the completed performance evaluation tracking spreadsheet for a sample of executive management members to determine that executive management evaluated the skills and expertise of its members annually.	No exceptions noted.
		Executive management maintains independence from those that operate the key controls implemented within the environment.	Inspected the organizational chart and the job description for a sample of job roles to determine that executive management maintained independence from those that operate the key controls implemented within the environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Executive management meets annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	Inspected the Leadership meeting minutes to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls implemented within the environment.	No exceptions noted.
		Executive management evaluates the skills and competencies of those that operate the internal controls implemented within the environment annually.	Inspected the completed performance and conduct evaluation for a sample of current employees to determine that executive management evaluated the skills and competencies of those that operate the internal controls implemented within the environment annually.	No exceptions noted.
		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 the operational management 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.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.	Inspected the organizational chart to determine that a documented organizational chart was in place that defined organizational structures, lines of reporting, and areas of authority.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities defined in written job descriptions consider and address specific requirements relevant to the system.	Inspected the job description for a sample of job roles to determine that roles and responsibilities defined in written job descriptions considered and addressed specific requirements relevant to the system.	No exceptions noted.
		A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the vendor management policy and standards and the completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Prior to employment, personnel are required to complete a background check.	Inspected the background check policy and procedure and the completed background check for a sample of new hires to determine that prior to employment, personnel were required to complete a background check.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance appraisals policy and the completed performance and conduct evaluation 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**
		Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	Inspected the performance appraisals and training program policies and procedures to determine that policies and procedures were in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		The entity evaluates the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.	Inspected the candidate evaluation for a sample of new hires to determine that the entity evaluated the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities.	No exceptions noted.
		The entity evaluates the competencies and experience of third-parties prior to working with them.	Inspected the compliance certifications for a sample of third-parties to determine that the entity evaluated the competencies and experience of third-parties prior to working with them.	No exceptions noted.
		Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer process.	Inspected the job description for a sample of job roles and interview notes for a sample of new hires to determine that job requirements were documented in the job descriptions and candidates' abilities to meet these requirements were evaluated as part of the hiring or transfer process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Environment				
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives.	Inspected the recruiting policies and procedures to determine that the entity had a recruiting department that was responsible for attracting individuals with competencies and experience that aligned with the entity's goals and objectives.	No exceptions noted.
		Employees are required to attend continued training annually that relates to their job role and responsibilities.	Inspected the Continued Professional Education (CPE) training tracker and training completion certificates for a sample of current employees to determine that employees were required to attend continued training annually that relates to their job role and responsibilities.	No exceptions noted.
		Executive management has created a training program for its employees.	Inspected the written information security policy and the training program policy and procedure to determine that executive management had created a training program for its employees.	No exceptions noted.
		Executive management uses an outside vendor to assist with its continued training of employees.	Inspected the third-party security awareness programs to determine that executive management used an outside vendor to assist with its continued training of employees.	No exceptions noted.
		Executive management tracks and monitors compliance with CPE training requirements.	Inspected the CPE training tracker to determine that executive management tracked and monitored compliance with CPE training requirements.	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**
		As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations and performs disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	Inspected the performance appraisals policy to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations and performed disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	No exceptions noted.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance appraisals policy and the completed performance and conduct evaluation 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 policy 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 intranet site.	Inspected the job description for a sample of job roles and the entity's intranet site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet 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 performance evaluation process as well as the competency and training requirements for personnel.	Inspected the performance appraisals and training program policies and procedures to determine that policies and procedures were in place that outline the performance evaluation process as well as the competency and training requirements for personnel.	No exceptions noted.
		As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations and performs disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	Inspected the performance appraisals policy to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations and performed disciplinary actions for its employees who do not meet expectations as it relates to their job role and responsibilities.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Network diagrams and data flow procedures are documented and maintained by management to identify the relevant internal and external information sources of the system.	Inspected the network diagrams and the data classification procedures to determine that network diagrams and data flow procedures were documented and maintained by management to identify the relevant internal and external information sources of the system.	No exceptions noted.
		Data hosted by the system is protected from unauthorized access.	Inspected the IDS configurations and the encryption methods and configurations to determine that data hosted by the system was protected from unauthorized access.	No exceptions noted.
		Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet site.	Inspected the written information security program and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's intranet site.	No exceptions noted.
		Data entered into the system, processed by the system and output from the system is protected from unauthorized access.	Inspected the IDS configurations and the encryption methods and configurations to determine that data entered into the system, processed by the system and output from the system was protected from unauthorized access.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Data is only retained for as long as required to perform the required system functionality, service or use.	Inspected the data retention and destruction policy 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.	Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.	Inspected the signed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that upon hire, personnel were required to acknowledge the employee handbook and code of conduct.	No exceptions noted.
		Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.	Inspected the signed employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook and code of conduct on an annual basis.	No exceptions noted.
		An anonymous channel is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Inspected the whistleblower reporting site and the anonymous reporting form to determine that an anonymous channel was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior.	Inspected the whistleblower reporting site and the anonymous reporting form to determine that employees, third-parties, and customers were directed on how to report unethical behavior.	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 intranet site.	Inspected the job description for a sample of job roles and the entity's intranet site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet site.	No exceptions noted.
		The entity's policies and procedures, code of conduct and employee handbook are made available to employees through the entity's intranet site.	Inspected the entity's intranet 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 site.	No exceptions noted.
		Upon hire, employees are required to complete information security awareness training.	Inspected the information security awareness training completion record for a sample of new hires to determine that upon hire, employees were required to complete information security awareness training.	No exceptions noted.
		Current employees are required to complete information security awareness training annually.	Inspected the information security awareness training completion record for a sample of current employees to determine that current employees were required to complete information security awareness training on an annual basis.	No exceptions noted.
		Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.	Inspected the Leadership 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.

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**
		Changes to job roles and responsibilities are communicated to personnel through the entity's intranet site.	Inspected the intranet site to determine that changes to job roles and responsibilities were communicated to personnel through the entity's intranet site.	No exceptions noted.
		Documented escalation procedures for reporting failures, incidents, concerns and other complaints are in place and made available to employees through the entity's intranet site.	Inspected the incident response policies and procedures and the entity's intranet 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 intranet site.	No exceptions noted.
		The entity's objectives, including changes made to the objectives, are communicated to its personnel through the entity's intranet site.	Inspected the entity's intranet site to determine that the entity's objectives, including changes made to the objectives, were communicated to its personnel through the entity's intranet site.	No exceptions noted.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	An anonymous channel is in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	Inspected the whistleblower reporting site and the anonymous reporting form to determine that an anonymous channel was in place to allow employees, third-parties, and customers to report unethical behavior in a confidential manner.	No exceptions noted.
		Employees, third-parties, and customers are directed on how to report unethical behavior.	Inspected the whistleblower reporting site and the anonymous reporting form to determine that employees, third-parties, and customers were directed on how to report unethical behavior.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Documented escalation procedures for reporting failures, incidents, concerns and other complaints are in place and made available to employees through the entity's intranet site.	Inspected the incident response policies and procedures and the entity's intranet 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 intranet site.	No exceptions noted.
		The entity's reviews that the third-party agreement delineate the boundaries of the system and describes relevant system components.	Inspected the master third-party agreement and the executed third-party agreement for a sample of third-parties to determine that the entity reviewed that the third-party agreement delineated the boundaries of the system and described relevant system components.	No exceptions noted.
		The entity reviews that the third-party agreement communicates the system commitments and requirements of third-parties.	Inspected the master third-party agreement and the executed third-party agreement for a sample of third-parties to determine that the entity reviewed that the third-party agreement communicated the system commitments and requirements of third-parties.	No exceptions noted.
		The entity reviews that the third-party agreement outlines and communicates the terms, conditions and responsibilities of third-parties.	Inspected the master third-party agreement and the executed third-party agreement for a sample of third-parties to determine that the entity reviewed that the third-party agreement outlined and communicated the terms, conditions and responsibilities of third-parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity's contractor agreement outlines and communicates the terms, conditions and responsibilities of external users.	Inspected the master contractor agreement to determine that the entity's contractor agreement outlined and communicated the terms, conditions and responsibilities of external users.	No exceptions noted.
		Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.	Inspected the master customer agreement and the executed customer agreement for a sample of customers to determine that customer commitments, requirements and responsibilities were outlined and communicated through service agreements.	No exceptions noted.
		Changes to commitments, requirements and responsibilities are communicated to third-parties, external users, and customers via updated agreements.	Inspected the updated services agreement to determine that changes to commitments, requirements and responsibilities were communicated to third-parties, external users and customers via updated agreements.	No exceptions noted.
		Executive management meets annually with operational management to discuss the results of assessments performed by third-parties.	Inspected the Leadership meeting minutes to determine that executive management met annually with operational management to discuss the results of assessments performed by third-parties.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Information and Communication				
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The entity communicates to external parties, vendors and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.	Inspected the master third-party agreement to determine that the entity communicated to external parties, vendors and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the Leadership meeting minutes and the risk management policies and procedures to determine that executive management reviewed and addressed repeated control failures.	No exceptions noted.
			Inspected the associated incident ticket for an example internal control that had failed to determine that executive management reviewed and addressed repeated control failures.	Testing of the control activity disclosed that no control failures occurred during the review period.
		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 organizational chart and the job description for responsible parties 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 had 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 performance appraisals policy, 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 and documented objectives and strategies to determine that business plans aligned with the entity's strategies and objectives.	No exceptions noted.
		Entity strategies, objectives and budgets are assessed on a quarterly basis.	Inspected the business plans and priorities meeting minutes for a sample of quarters to determine that entity strategies, objectives and budgets were assessed on a quarterly basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Documented policies and procedures are in place to guide personnel when performing a risk assessment.	Inspected the risk assessment and management policies and procedures to determine that documented policies and procedures were in place to guide personnel when performing a risk assessment.	No exceptions noted.
		Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	Inspected the risk assessment and management policies and procedures to determine that management defined a formal risk assessment process that specified the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.	No exceptions noted.
		A formal risk assessment is performed on 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 the completed risk assessment to determine that the entity's risk assessment process included: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks 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 the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		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 to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures and the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 the completed risk assessment to determine that for gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, were assigned to process owners based on roles and responsibilities.	No exceptions noted.
		The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.	Inspected the risk assessment policy and procedure and the completed risk assessment to determine that the annual comprehensive risk assessment results were reviewed and approved by appropriate levels of management.	No exceptions noted.
		As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third-parties.	Inspected the risk assessment policy and procedure and the 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.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.	Inspected the completed risk 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.

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 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 risk assessment to determine that as part of management's assessment of fraud risks, management considered key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities.	Inspected the completed fraud assessment to determine that as part of management's assessment of fraud risks, management considered how personnel could engage in or justify fraudulent activities.	No exceptions noted.
		As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT.	Inspected the completed fraud assessment to determine that as part of management's assessment of fraud risks, management considered threats and vulnerabilities that arise from the use of IT.	No exceptions noted.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Assessment				
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Changes in vendor and third-party relationships are considered and evaluated as part of the annual comprehensive risk assessment.	Inspected the risk assessment policy and procedure and the completed risk assessment to determine that changes in vendor and third-party relationships were considered and evaluated as part of the annual comprehensive risk assessment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring system configurations, the centralized antivirus software dashboard console, and the IDS configurations 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.
		Performance and conduct evaluations are performed for personnel on an annual basis.	Inspected the performance appraisals policy and the completed performance and conduct evaluation for a sample of current employees to determine that performance and conduct evaluations were performed for personnel on an annual basis.	No exceptions noted.
		A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	Inspected the completed risk assessment to determine that a formal risk assessment was performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.	No exceptions noted.
		Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.	Inspected the entity policies and procedures and Leadership meeting minutes to determine that management reviewed policies, procedures and other control documents for accuracy and applicability on an annual basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 Leadership meeting minutes and 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.
		Logical access reviews are performed monthly.	Inquired of the VP of Technology Services regarding user access reviews to determine that logical access reviews were performed monthly.	No exceptions noted.
			Inspected the completed logical access reviews for a sample of months to determine that logical access reviews were performed monthly.	No exceptions noted.
		Vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities.	Inspected the vulnerability scanning policy and the completed vulnerability scan results for a sample of months to determine that vulnerability scans were performed monthly on the environment to identify control gaps and vulnerabilities.	No exceptions noted.
		A third-party performs an external vulnerability scan monthly to identify and exploit vulnerabilities identified within the environment.	Inspected the completed vulnerability scan results for a sample of months to determine that a third-party performed an external vulnerability scan monthly 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 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.
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.	Backup restoration tests are performed on an annual basis.	Inspected the completed backup restoration test results to determine that backup restoration tests were performed on an annual basis.	No exceptions noted.
		Management obtains and reviews attestation reports of critical vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation report review for a sample of critical vendors and third-parties to determine that management obtained and reviewed attestation reports of critical vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
		Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	Inspected the Leadership meeting minutes to determine that senior management was made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Vulnerabilities identified from the various assessments performed on the environment are communicated to those parties responsible for taking corrective actions.	Inspected the risk assessment, the internal vulnerability scan results performed on the environment and the supporting incident tickets for a sample of vulnerabilities identified from a vulnerability scan to determine that vulnerabilities identified from the various assessments performed on the environment were communicated to those parties responsible for taking corrective actions.	No exceptions noted.
		Vulnerabilities identified from the various assessments performed on the environment are documented, investigated, and addressed.	Inspected the risk assessment, the internal vulnerability scan results performed on the environment and the supporting incident tickets for a sample of vulnerabilities identified from a vulnerability scan to determine that vulnerabilities identified from the various assessments performed on the environment were documented, investigated and addressed.	No exceptions noted.
		Vulnerabilities, deviations, and control gaps identified from the risk and compliance assessments are tracked, documented, investigated, addressed and communicated to those parties responsible for taking corrective actions.	Inquired of the VP of Technology Services regarding the vulnerability management process to determine that vulnerabilities, deviations, and control gaps identified from the risk and compliance assessments were tracked, documented, investigated, addressed and communicated to those parties responsible for taking corrective actions.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Monitoring Activities				
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the risk assessment policies and procedures and the vulnerability scanning policy to determine that vulnerabilities, deviations, and control gaps identified from the risk and compliance assessments were required to be tracked, documented, investigated, addressed and communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting remediation ticket for a sample of vulnerabilities to determine that vulnerabilities, deviations, and control gaps identified from the risk and compliance assessments were tracked, documented, investigated, addressed, and communicated to those parties responsible for taking corrective actions.	No exceptions noted.
			Inspected the supporting remediation ticket for a sample of deviations and control gaps to determine that vulnerabilities, deviations, and control gaps identified from the risk and compliance assessments were tracked, documented, investigated, addressed, and communicated to those parties responsible for taking corrective actions.	Testing of the control activity disclosed that no deviations or control gaps occurred during the review period.

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

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures and the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	Inspected the completed risk assessment to determine that as part of the risk assessment process, controls within the environment were modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.	No exceptions noted.
		Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	Inquired of the VP of Technology Services regarding the internal controls process to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the risk assessment policies and procedures and the vulnerability scanning policy to determine that controls within the environment were required to be modified and implemented to mitigate vulnerabilities, deviations and control 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**
			Inspected the supporting remediation ticket for a sample of vulnerabilities to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	No exceptions noted.
			Inspected the supporting remediation ticket for a sample of deviations and control gaps to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.	Testing of the control activity disclosed that no deviations or control gaps occurred during the review period.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.	Inspected the 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 and disaster recovery plans to determine that business continuity and disaster recovery plans were developed and updated on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		An analysis of incompatible operational duties is performed on an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the key personnel review to determine that an analysis of incompatible operational duties was performed on an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	No exceptions noted.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet site.	Inspected the written information security program and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's intranet site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Management has 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 had 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 had documented the controls implemented around the entity's technology infrastructure.	No exceptions noted.
		Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.	Inspected the 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The internal controls implemented around the entity's technology infrastructure include, but are not limited to: • Restricting access rights to authorized users • Authentication of access • Protecting the entity's assets from external threats • Limiting services to what is required for business operations	Inspected the completed internal controls matrix and the written information security program 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 • Limiting services to what is required for business operations	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 had established controls around the acquisition, development and maintenance of the entity's technology infrastructure.	No exceptions noted.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet site.	Inspected the job description for a sample of job roles and the entity's intranet site to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet site.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's intranet site.	Inspected the written information security program and the entity's intranet to determine that organizational and information security policies and procedures were documented and made available to personnel through the entity's intranet site.	No exceptions noted.
		Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.	Inspected the organizational chart and the 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.
		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.
		Process owners and management investigate and troubleshoot control failures.	Inquired of the Chief Executive Officer regarding control failures to determine that process owners and management were required to investigate and troubleshoot control failures.	No exceptions noted.
			Inspected the completed risk assessment to determine that process owners and management investigated and troubleshot control failures.	No exceptions noted.
			Inspected the associated incident ticket for an example internal control that had failed to determine that process owners and management investigated and troubleshot control failures.	Testing of the control activity disclosed that no control failures occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Control Activities				
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The effectiveness of the internal controls implemented within the environment is evaluated annually.	Inspected the Leadership meeting minutes and the completed internal controls matrix to determine that the effectiveness of the internal controls implemented within the environment was evaluated annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Backup restoration tests are performed on an annual basis.	Inspected the completed backup restoration test results to determine that backup restoration tests were performed on an annual basis.	No exceptions noted.
		Critical data is stored in encrypted format using Oracle-managed encryption keys.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using Oracle-managed encryption keys.	No exceptions noted.
		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 written information security policies 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 VP of Technology Services regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

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 user access is restricted via role-based security privileges defined within the access control system.	Inquired of the VP of Technology Services regarding network user access to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
			Inspected the network user listing and access rights to determine that network user access was restricted via role-based security privileges defined within the access control system.	No exceptions noted.
		Network administrative access is restricted to user accounts accessible by authorized personnel.	Inquired of the VP of Technology Services regarding network administrative access to determine that network administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
			Inspected the network administrator listing and access rights to determine that network administrative access was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
		Network users are authenticated via individually assigned user accounts, passwords and multi-factor authentication (MFA).	Inquired of the VP of Technology Services regarding network user access to determine that network users were authenticated via individually assigned user accounts, passwords and MFA.	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**
			Observed a user login to the network to determine that network users were authenticated via individually assigned user accounts, passwords and MFA.	No exceptions noted.
			Inspected the network user listing and password configurations to determine that network users were authenticated via individually assigned user accounts and passwords.	No exceptions noted.
		The networks are configured to enforce password requirements that include: • Password history • Password age • Password length • Complexity	Inspected the network password settings to determine that the networks were configured to enforce password requirements that included: • Password history • 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.

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 logging configurations are in place that include user activity and 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 user activity and system events.	No exceptions noted.
		Network audit logging settings are in place for system events and logs are maintained and reviewed as needed.	Inquired of the VP of Technology Services regarding network audit logs to determine that network audit logging settings were in place for system events and logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected the network audit logging configurations and an example log extract to determine that network audit logging settings were in place for system events and logs were maintained and reviewed as needed.	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 networks listings 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, the firewall configurations 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 digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Encryption keys are protected during generation, storage, use, and destruction.	Inquired of the VP of Technology Services regarding the encryption keys to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
			Inspected the encryption policies and procedures to determine that encryption keys were required to be protected during generation, storage, use, and destruction.	No exceptions noted.
		Logical access reviews are performed monthly.	Inquired of the VP of Technology Services 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 Chief Executive Officer 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 access control policies and procedures, the onboarding policies and procedures and the supporting onboarding ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.
		Logical access to systems is revoked for an employee as a component of the termination process.	Inquired of the Chief Executive Officer 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 access control policies and procedures, the termination policies and procedures and the supporting offboarding ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.

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**
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the VP of Technology Services regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Backup restoration tests are performed on an annual basis.	Inspected the completed backup restoration test results to determine that backup restoration tests were performed on an annual basis.	No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the written information security policies 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 VP of Technology Services regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the listings of privileged users to the network 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 VP of Technology Services 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 Chief Executive Officer 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 access control policies and procedures, the onboarding policies and procedures and the supporting onboarding ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access to systems is revoked for an employee as a component of the termination process.	Inquired of the Chief Executive Officer 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 access control policies and procedures, the termination policies and procedures and the supporting offboarding ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the VP of Technology Services 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**
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	An analysis of incompatible operational duties is performed on an annual basis, and where incompatible responsibilities are identified, compensating controls are put into place.	Inspected the key personnel review to determine that an analysis of incompatible operational duties was performed on an annual basis, and where incompatible responsibilities were identified, compensating controls were put into place.	No exceptions noted.
		Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.	Inspected the written information security policies 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 VP of Technology Services regarding privileged access to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
			Inspected the listings of privileged users to the network to determine that privileged access to sensitive resources was restricted to authorized personnel.	No exceptions noted.
		Network user access is restricted via role-based security privileges defined within the access control system.	Inquired of the VP of Technology Services regarding network user 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.
		Logical access reviews are performed monthly.	Inquired of the VP of Technology Services 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 Chief Executive Officer 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 access control policies and procedures, the onboarding policies and procedures and the supporting onboarding ticket for a sample of new hires to determine that logical access to systems was approved and granted to an employee as a component of the hiring process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Logical access to systems is revoked for an employee as a component of the termination process.	Inquired of the Chief Executive Officer 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 access control policies and procedures, the termination policies and procedures and the supporting offboarding ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
		Privileged access to add, remove, or modify access to user accounts is restricted to authorized personnel.	Inquired of the VP of Technology Services regarding privileged access to sensitive resources to determine that privileged access to sensitive resources add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.
			Inspected the listing of privileged users to the in-scope systems to determine that privileged access to add, remove, or modify access to user accounts was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Logical access to systems is revoked for an employee as a component of the termination process.	Inquired of the Chief Executive Officer 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 access control policies and procedures, the termination policies and procedures and the supporting offboarding ticket for a sample of terminated employees to determine that logical access to systems was revoked for an employee as a component of the termination process.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Data that is no longer required for business purposes is rendered unreadable.	Inquired of the VP of Technology Services regarding the data disposal process to determine that data that was no longer required for business purposes was rendered unreadable.	No exceptions noted.
			Inspected the data retention and destruction policy and procedures to determine that data that was no longer required for business purposes was rendered unreadable.	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 service ticket and certificate of destruction 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 for business purposes was rendered unreadable.	Testing of the control activity disclosed that no data disposals occurred during the review period.
		Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.	Inspected the data disposal and destruction policies and procedures to determine that policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction.	No exceptions noted.
		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.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Critical data is stored in encrypted format using Oracle-managed encryption keys.	Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using Oracle-managed encryption keys.	No exceptions noted.
		A DMZ is in place to isolate outside access and data from the entity's environment.	Inspected the DMZ settings to determine that a DMZ was in place to isolate outside access and data from the entity's environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		Network address translation (NAT) functionality is utilized to manage internal IP addresses.	Inspected the NAT gateways configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations for data in transit to determine that TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the VP of Technology Services regarding access to stored data to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.
			Inspected the Oracle Cloud Infrastructure (OCI) user listing to determine that logical access to stored data was restricted to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A firewall is in place to filter unauthorized inbound network traffic from the Internet.	Inspected the network diagram, the firewall configurations and the firewall rulesets for a sample of production virtual desktops 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, the firewall configurations and the firewall rulesets for a sample of production virtual desktops 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 intrusion detection system (IDS) is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and the 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 notification configurations and an example IDS alert notification e-mail 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 production virtual workspaces to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the centralized antivirus software dashboard console and the antivirus configurations for a sample of workstations and production virtual workspaces to determine that antivirus software was installed on workstations and production virtual workspaces to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus software dashboard console and the antivirus software configurations for a sample of workstations and production virtual workspaces 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 production virtual workspaces on a daily basis.	Inspected the centralized antivirus software dashboard console and the antivirus software configurations for a sample of workstations and production virtual workspaces to determine that the antivirus software was configured to scan workstations and production virtual workspaces on a daily basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Logical and Physical Access Controls				
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Use of removable media is prohibited by policy except when authorized by management.	Inspected the removable media policies and procedures to determine that the use of removable media was prohibited by policy except when authorized by management.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.	Inspected the encryption configurations for data in transit and digital certificates to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.	No exceptions noted.
		NAT functionality is utilized to manage internal IP addresses.	Inspected the NAT gateways configurations to determine that NAT functionality was utilized to manage internal IP addresses.	No exceptions noted.
		TLS and other encryption technologies are used for defined points of connectivity.	Inspected the encryption configurations for data in transit to determine that TLS and other encryption technologies were used for defined points of connectivity.	No exceptions noted.
		Transmission of digital output beyond the boundary of the system is encrypted.	Inspected the encryption configurations for data in transit and digital certificates to determine that transmission of digital output beyond the boundary of the system was encrypted.	No exceptions noted.
		Logical access to stored data is restricted to authorized personnel.	Inquired of the VP of Technology Services 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 OCI user listing 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, the firewall configurations and the firewall rulesets for a sample of production virtual desktops 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, the firewall configurations and the firewall rulesets for a sample of production virtual desktops 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 the 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 notification configurations and an example IDS alert notification e-mail 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**
		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.
		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.
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.	Antivirus software is installed on workstations and production virtual workspaces to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the centralized antivirus software dashboard console and the antivirus configurations for a sample of workstations and production virtual workspaces to determine that antivirus software was installed on workstations and production virtual workspaces to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus software dashboard console and the antivirus software configurations for a sample of workstations and production virtual workspaces 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.

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 is configured to scan workstations and production virtual workspaces on a daily basis.	Inspected the centralized antivirus software dashboard console and the antivirus software configurations for a sample of workstations and production virtual workspaces to determine that the antivirus software was configured to scan workstations and production virtual workspaces on a daily basis.	No exceptions noted.
		The ability to install applications and software on workstations is restricted to authorized personnel.	Inquired of the VP of Technology Services 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.
		Access to implement changes in the production environment is restricted to authorized IT personnel.	Inquired of the VP of Technology Services regarding access to implement changes in the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
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 list of administrators with access to implement changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		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.

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 system configurations, the centralized antivirus software dashboard console, and the IDS configurations 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.
		Vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities.	Inspected the vulnerability scanning policy and the completed vulnerability scan results for a sample of months to determine that vulnerability scans were performed monthly on the environment to identify control gaps and vulnerabilities.	No exceptions noted.
		A third-party performs an external vulnerability scan monthly to identify and exploit vulnerabilities identified within the environment.	Inspected the completed vulnerability scan results for a sample of months to determine that a third-party performed an external vulnerability scan monthly 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, the firewall configurations and the firewall rulesets for a sample of production virtual desktops 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, the firewall configurations and the firewall rulesets for a sample of production virtual desktops 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 the 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 notification configurations and an example IDS alert notification e-mail 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.
		Management defined configuration standards in the information security policies and procedures.	Inspected the written information security program to determine that management defined configuration standards in the information security policies and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the written information security program and the incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.	Inspected the monitoring system configurations, the centralized antivirus software dashboard console, and the IDS configurations 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Network audit logging configurations are in place that include user activity and 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 user activity and system events.	No exceptions noted.
		Network audit logging settings are in place for system events and logs are maintained and reviewed as needed.	Inquired of the VP of Technology Services regarding network audit logs to determine that network audit logging settings were in place for system events and logs were maintained and reviewed as needed.	No exceptions noted.
			Inspected the network audit logging configurations and an example log extract to determine that network audit logging settings were in place for system events and logs were maintained and reviewed as needed.	No exceptions noted.
		An IDS is utilized to analyze network events and report possible or actual network security breaches.	Inspected the network diagram and the 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 notification configurations and an example IDS alert notification e-mail 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 production virtual workspaces to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.	Inspected the centralized antivirus software dashboard console and the antivirus configurations for a sample of workstations and production virtual workspaces to determine that antivirus software was installed on workstations and production virtual workspaces to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.	No exceptions noted.
		The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.	Inspected the centralized antivirus software dashboard console and the antivirus software configurations for a sample of workstations and production virtual workspaces 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 production virtual workspaces on a daily basis.	Inspected the centralized antivirus software dashboard console and the antivirus software configurations for a sample of workstations and production virtual workspaces to determine that the antivirus software was configured to scan workstations and production virtual workspaces on a daily basis.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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.
		Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	Inspected the written information security program and the incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.	No exceptions noted.
		Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	Inspected the incident 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 Leadership 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.

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 policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.	No exceptions noted.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident response policies and procedures to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		The incident response policies and procedures define the classification of incidents based on its severity.	Inspected the incident response policies and procedures to determine that the incident response policies and procedures defined the classification of incidents based on its severity.	No exceptions noted.
		Resolution of incidents are documented and tracked in a standardized ticketing system, identified incidents are reviewed, monitored and investigated by an incident response team, and communicated to affected users.	Inspected the supporting incident ticket for a sample of non-critical security incidents to determine that the resolution of incidents was documented and tracked in a standardized ticketing system, identified incidents were reviewed, monitored and investigated by an incident response team, 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 actions taken to address identified security incidents are documented and updated to reflect the planned incident and problem resolution and are communicated to affected parties.	Inspected the supporting incident ticket for a sample of non-critical security incidents to determine that the incidents were documented and tracked in a standardized ticketing system and actions taken to address identified security incidents were documented and updated to reflect the planned incident and problem resolution and were communicated to affected parties.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the VP of Technology Services regarding security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that a security incident analysis was required to be performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incidents to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Identified incidents are reviewed, monitored and investigated by an incident response team.	Inspected the supporting incident ticket for a sample of non-critical security incidents to determine that identified incidents were reviewed, monitored and investigated by an incident response team.	No exceptions noted.
		Incidents resulting in the unauthorized use or disclosure of personal information are communicated to the affected users.	Inquired of the VP of Technology Services regarding security incidents to determine that incidents resulting in the unauthorized use or disclosure of personal information were required to be communicated to the affected users.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that incidents resulting in the unauthorized use or disclosure of personal information were required to be communicated to the affected users.	No exceptions noted.
			Inspected the supporting incident ticket for an example critical security incident that resulted in unauthorized disclosure of personal information to determine that incidents resulting in the unauthorized use or disclosure of personal information were identified and communicated to the affected users.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
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 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 Leadership meeting minutes to determine that management reviewed reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identified the need for system changes and implementation of additional controls based on incident patterns and root causes.	No exceptions noted.
		The incident response and escalation procedures are reviewed at least annually for effectiveness.	Inspected the revision history of the incident response policies and procedures to determine that the incident response and escalation procedures were reviewed at least annually for effectiveness.	No exceptions noted.
		Resolution of incidents are documented and tracked in a standardized ticketing system, identified incidents are reviewed, monitored and investigated by an incident response team, and communicated to affected users.	Inspected the supporting incident ticket for a sample of non-critical security incidents to determine that the resolution of incidents was documented and tracked in a standardized ticketing system, identified incidents were reviewed, monitored and investigated by an incident response team, 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 actions taken to address identified security incidents are documented and updated to reflect the planned incident and problem resolution and are communicated to affected parties.	Inspected the supporting incident ticket for a sample of non-critical security incidents to determine that the incidents were documented and tracked in a standardized ticketing system and actions taken to address identified security incidents were documented and updated to reflect the planned incident and problem resolution and were communicated to affected parties.	No exceptions noted.
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the VP of Technology Services regarding security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that a security incident analysis was required to be performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incidents to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.	Inspected the incident response policies and procedures to determine that roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program were defined and documented.	No exceptions noted.
		The actions taken to address identified security incidents are documented and communicated to affected parties.	Inspected the supporting incident ticket for a sample of non-critical security incidents to determine that the actions taken to address identified security incidents were documented and communicated to affected parties.	No exceptions noted.
		Documented incident response and escalation procedures are in place to guide personnel in addressing the threats posed by security incidents.	Inspected the incident response policies and procedures to determine that documented incident response and escalation procedures were in place to guide personnel in addressing the threats posed by security incidents.	No exceptions noted.
		Critical security incidents that result in a service/business operation disruption are communicated to those affected through the creation of a ticket.	Inquired of the VP of Technology Services regarding security incidents to determine that critical security incidents that resulted in a service/business operation disruption were communicated to those affected through the creation of a ticket.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
			Inspected the incident response policies and procedures to determine that critical security incidents that resulted in a service/business operation disruption were required to be communicated to those affected through the creation of a ticket.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incidents that resulted in a service/business operation disruption to determine that critical security incidents that resulted in a service/business operation disruption were communicated to those affected through the creation of a ticket.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.
		Remediation actions taken for security incidents are documented within the ticket and communicated to affected users.	Inspected the supporting incident ticket for a sample of non-critical security incidents to determine that the remediation actions taken for security incidents were documented within the ticket and communicated to affected users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		The risks associated with identified vulnerabilities are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk	Inspected the supporting incident ticket for a sample of vulnerabilities identified from a vulnerability scan 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.	Backup restoration tests are performed on an annual basis.	Inspected the completed backup restoration test results to determine that backup restoration tests were performed on an annual basis.	No exceptions noted.
		Business continuity and disaster recovery plans are tested on an annual basis.	Inspected the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plans were tested on an annual basis.	No exceptions noted.
		Management reviews reports on an annual basis summarizing incidents, root cause of incidents, and corrective action plans and as part of the review, management identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.	Inspected the Leadership 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.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
System Operations				
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.	Inquired of the VP of Technology Services regarding security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the incident response policies and procedures to determine that a security incident analysis was required to be performed for critical incidents to determine the root cause, system impact and resolution.	No exceptions noted.
			Inspected the supporting incident ticket for a sample of critical security incidents to determine that an impact analysis was performed to determine the root cause, system impact, and resolution.	Testing of the control activity disclosed that no critical security incidents occurred during the review period.
		Change management requests are opened for incidents that require permanent fixes.	Inspected the written information security program and 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**
		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 written information security program, the incident response policies and procedures, and the change management policies and procedures, and the system build guides for critical systems to determine that the entity restored system operations for incidents impacting the environment through activities that included, but were not limited to: • Rebuilding systems • Updating software • Installing patches • Removing unauthorized access • Changing configurations	No exceptions noted.
		Data backup and restore procedures are in place to guide personnel in performing backup activities.	Inspected the backup policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities.	No exceptions noted.
		A business continuity and disaster recovery plan is documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.	Inspected the business continuity and disaster recovery plans to determine that a business continuity and disaster recovery plan was documented to identify and reduce risks, limited the consequences of damaging incidents, and ensured the timely resumption of essential operations.	No exceptions noted.

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 the completed business continuity and disaster recovery test results to determine that the business continuity and disaster recovery plan and procedures were updated based on disaster recovery plan test results.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Access to implement changes in the production environment is restricted to authorized IT personnel.	Inquired of the VP of Technology Services regarding access to implement changes in the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
			Inspected the list of administrators with access to implement changes into the production environment to determine that access to implement changes in the production environment was restricted to authorized IT personnel.	No exceptions noted.
		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.

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**
		The change management process has defined the following roles and assignments: • Authorization of change requests - customer, owner, or reporter • Development - development team and data owners • Testing - asset custodians and data owners • Approver - approver group • Implementation - OCI Admin • Verification - asset custodians and validator group	Inspected the change management policies and procedures to determine that the change management process defined the following roles and assignments: • Authorization of change requests - customer, owner, or reporter • Development - development team and data owners • Testing - asset custodians and data owners • Approver - approver group • Implementation - OCI Admin • Verification - asset custodians and validator group	No exceptions noted.
		System changes are communicated to both affected internal and external users.	Inspected the external change communication via e-mail and the internal change communication via change tickets to determine that system changes were communicated to both affected internal and external users.	No exceptions noted.
		System changes are authorized and approved prior to implementation.	Inspected the supporting change ticket for a sample of system changes to determine that system changes were authorized and approved prior to implementation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		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 rollback repository to determine that prior code was held in the source code repository for rollback capability in the event that a system change did not function as designed.	No exceptions noted.
		System patches/security updates follow the standard change management process.	Inspected the patch management policies and procedures to determine that system patches/security updates follow the standard patch management process.	No exceptions noted.
		System patches/security updates are performed on a configured schedule.	Inspected the supporting tickets for a sample of system patches to determine that system patches/security updates were performed on a configured schedule.	No exceptions noted.
		Development and test environments are physically and logically separated from the production environment.	Inspected the separate development and production environments to determine that development and test environments were physically and logically separated from the production environment.	No exceptions noted.
		System change requests are documented and tracked in a ticketing system.	Inspected the supporting change ticket for a sample of system changes to determine that system change requests were documented and tracked in a ticketing system.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Back out procedures are documented to allow for rollback of application changes when changes impaired system operations.	Inspected the rollback plan checklist and the rollback repository to determine that back out procedures were documented to allow for rollback of application changes when changes impaired system operation.	No exceptions noted.
		A code/peer review is systematically required prior to deploying the Pull Request (PR) into the production environment.	Inspected the supporting change ticket for a sample of system changes to determine that a code/peer review was systematically required prior to deploying the PR into the production environment.	No exceptions noted.
		System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.	Inspected the supporting change ticket for a sample of 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.
		System changes implemented for remediating incidents follow the standard change management process.	Inspected the change management policies and procedures and the supporting change ticket for a sample of non-critical security incidents to determine that system changes implemented for remediating incidents followed the standard change management process.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Change Management				
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.	Inspected the written information security program to determine that information security policies and procedures documented the baseline requirements for configuration of IT systems and tools.	No exceptions noted.
		Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.	Inspected the change management policies and procedures to determine that documented change control policies and procedures were in place to guide personnel in implementing changes in an emergency situation.	No exceptions noted.

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

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 to address risks identified during the risk assessment process.	Inspected the risk assessment and management policies and procedures and the completed risk assessment to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
		Documented policies and procedures are in place to guide personnel in performing risk assessment and risk mitigation activities.	Inspected the risk assessment and management policies and procedures to determine that documented policies and procedures were in place to guide personnel in performing risk assessment and risk mitigation activities.	No exceptions noted.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY				
Risk Mitigation				
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**	**Test Applied by the Service Auditor**	**Test Results**
		Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.	Inspected the vendor risk assessment policies and procedures and the completed risk assessment to determine that identified risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third-parties.	Inspected the vendor management policy and standards and the completed vendor risk assessment to determine that a vendor risk assessment was performed on an annual basis which included reviewing the activities performed by third-parties.	No exceptions noted.
		Management obtains and reviews attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	Inspected the completed third-party attestation reports for a sample of third-parties that the entity has a relationship with to determine that management obtained and reviewed attestation reports and vendor questionnaires of vendors and third-parties to evaluate the effectiveness of controls within the vendor or third-party's environment.	No exceptions noted.
		The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the insurance documentation to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	No exceptions noted.

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

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

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