



A-LIGN

the business unit
gtechna, a business unit
of Acceo Solutions Inc., a
Corporation under the
Canada Corporations Act
and it's U.S. affiliate,
GTECHNA USA
CORPORATION

Type 2 SOC 2

2023

gtechna[•]



**REPORT ON THE BUSINESS UNIT GTECHNA, A BUSINESS UNIT OF ACCEO
SOLUTIONS INC., A CORPORATION UNDER THE CANADA CORPORATIONS
ACT AND IT'S U.S. AFFILIATE, GTECHNA USA CORPORATION'S
DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF
THE DESIGN AND OPERATING EFFECTIVENESS OF ITS
CONTROLS RELEVANT TO SECURITY**

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

October 1, 2022 to September 30, 2023

Table of Contents

| | |
|---|-----------|
| SECTION 1 ASSERTION OF THE BUSINESS UNIT GTECHNA, A BUSINESS UNIT OF ACCEO SOLUTIONS INC., A CORPORATION UNDER THE CANADA CORPORATIONS ACT AND IT'S U.S. AFFILIATE, GTECHNA USA CORPORATION MANAGEMENT | 1 |
| SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT | 4 |
| SECTION 3 THE BUSINESS UNIT GTECHNA, A BUSINESS UNIT OF ACCEO SOLUTIONS INC., A CORPORATION UNDER THE CANADA CORPORATIONS ACT AND IT'S U.S. AFFILIATE, GTECHNA USA CORPORATION'S DESCRIPTION OF ITS E-CITATION SOFTWARE SERVICES SYSTEM THROUGHOUT THE PERIOD OCTOBER 1, 2022 TO SEPTEMBER 30, 2023..... | 8 |
| OVERVIEW OF OPERATIONS..... | 9 |
| Company Background | 9 |
| Description of Services Provided | 9 |
| Principal Service Commitments and System Requirements..... | 10 |
| Components of the System..... | 10 |
| Boundaries of the System..... | 15 |
| RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING | 15 |
| Control Environment..... | 15 |
| Risk Assessment Process | 16 |
| Information and Communications Systems..... | 17 |
| Monitoring Controls | 17 |
| Changes to the System Since the Last Review..... | 18 |
| Incidents Since the Last Review | 18 |
| Criteria Not Applicable to the System | 18 |
| Subservice Organizations..... | 18 |
| COMPLEMENTARY USER ENTITY CONTROLS..... | 19 |
| TRUST SERVICES CATEGORIES..... | 20 |
| SECTION 4 TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS | 21 |
| GUIDANCE REGARDING TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS | 22 |
| CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION | 23 |
| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | 23 |

SECTION 1

ASSERTION OF THE BUSINESS UNIT GTECHNA, A BUSINESS UNIT OF ACCEO SOLUTIONS INC., A CORPORATION UNDER THE CANADA CORPORATIONS ACT AND IT'S U.S. AFFILIATE, GTECHNA USA CORPORATION MANAGEMENT

**ASSERTION OF THE BUSINESS UNIT GTECHNA, A BUSINESS UNIT OF ACCEO SOLUTIONS INC.,
A CORPORATION UNDER THE CANADA CORPORATIONS ACT AND IT'S U.S. AFFILIATE,
GTECHNA USA CORPORATION MANAGEMENT**

December 19, 2023

We have prepared the accompanying description of the business unit gtechna, a business unit of Acceo Solutions Inc., a Corporation under the Canada Corporations Act and it's U.S. affiliate, GTECHNA USA CORPORATION's ('gtechna' or 'the Company') e-Citation Software Services System titled "the business unit gtechna, a business unit of Acceo Solutions Inc., a Corporation under the Canada Corporations Act and it's U.S. affiliate, GTECHNA USA CORPORATION's Description of Its e-Citation Software Services System throughout the period October 1, 2022 to September 30, 2023" (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 e-Citation Software Services System that may be useful when assessing the risks arising from interactions with gtechna's system, particularly information about system controls that gtechna 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)*.

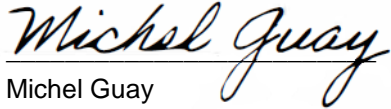
gtechna uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at gtechna, to achieve gtechna's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

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

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

- a. the description presents gtechna's e-Citation Software Services System that was designed and implemented throughout the period October 1, 2022 to September 30, 2023, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that gtechna'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 gtechna's controls throughout that period.

- c. the controls stated in the description operated effectively throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that gtechna'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 gtechna's controls operated effectively throughout that period.



Michel Guay

Executive Vice President

the business unit gtechna, a business unit of Acceo Solutions Inc., a Corporation under the Canada Corporations Act and it's U.S. affiliate, GTECHNA USA CORPORATION

SECTION 2
INDEPENDENT SERVICE AUDITOR'S REPORT



INDEPENDENT SERVICE AUDITOR'S REPORT

To: the business unit gtechna, a business unit of Acceo Solutions Inc., a Corporation under the Canada Corporations Act and it's U.S. affiliate, GTECHNA USA CORPORATION

Scope

We have examined gtechna's accompanying description of its e-Citation Software Services System titled "the business unit gtechna, a business unit of Acceo Solutions Inc., a Corporation under the Canada Corporations Act and it's U.S. affiliate, GTECHNA USA CORPORATION's Description of Its e-Citation Software Services System throughout the period October 1, 2022 to September 30, 2023" (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 October 1, 2022 to September 30, 2023, to provide reasonable assurance that gtechna'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*).

gtechna uses AWS 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 gtechna, to achieve gtechna's service commitments and system requirements based on the applicable trust services criteria. The description presents gtechna's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of gtechna's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

gtechna 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 gtechna's service commitments and system requirements were achieved. gtechna has provided the accompanying assertion titled "Assertion of the business unit gtechna, a business unit of Acceo Solutions Inc., a Corporation under the Canada Corporations Act and it's U.S. affiliate, GTECHNA USA CORPORATION Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. gtechna 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 gtechna's e-Citation Software Services System that was designed and implemented throughout the period October 1, 2022 to September 30, 2023, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that gtechna'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 gtechna's controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that gtechna'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 gtechna'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 gtechna, user entities of gtechna's e-Citation Software Services System during some or all of the period October 1, 2022 to September 30, 2023, business partners of gtechna subject to risks arising from interactions with the e-Citation Software Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

A-LIGN ASSURANCE

Tampa, Florida
December 19, 2023

SECTION 3

**THE BUSINESS UNIT GTECHNA, A BUSINESS UNIT OF ACCEO SOLUTIONS INC.,
A CORPORATION UNDER THE CANADA CORPORATIONS ACT AND IT'S U.S.
AFFILIATE, GTECHNA USA CORPORATION'S DESCRIPTION OF ITS
E-CITATION SOFTWARE SERVICES SYSTEM THROUGHOUT
THE PERIOD OCTOBER 1, 2022 TO SEPTEMBER 30, 2023**

OVERVIEW OF OPERATIONS

Company Background

gtechna develops e-Citation software to automate law enforcement and parking management, as well as civil code regulations for police, by-law, and public works departments in North America. For over 20 years, gtechna has developed lasting relationships with cities such as Pittsburgh, PA, Washington D.C., Baltimore, MD, Toronto Police Service, and Service de police de la Ville de Montréal police and parking divisions.

gtechna began as a small hi-tech start-up founded by two long-time university friends in 1992. As a result of the recent boom in the Information Technology (IT) sector, gtechna has become an award-winning enterprise software provider. gtechna's premier product line Officer™ Suite is increasingly becoming one of the most adopted citations software solutions in North America.

Description of Services Provided

Organizations across North America trust gtechna software because it streamlines the enforcement process from end to end.

From time-saving electronic citations with license plate recognition software, to easy online payments for customers, gtechna makes parking management process futureproof.

Enforcement activities can be complicated, but with gtechna, they don't have to be. The gtechna line of enforcement software streamlines the activities that tend to slow down and drain organization resources.

Police Departments

With built-in license plate recognition integration, gtechna mobile Police Ticketing helps officers enforce traffic laws and issue citations more efficiently.

Parking Authorities

gtechna Parking makes the most of agency's assets and provides a streamlined experience for parking agents and customers with cloud-based parking rights, citations, and payments for on street and off-street parking management.

Private Operators

A complete integrated solution with feature-rich modules that can be enlisted to meet off-street needs for lots and garages. From the most sophisticated too simple in-out access control, the gateless solutions - or gate assisted integration - are optimized for inventory, digital signage, payment, and enforcement to maximize compliance, eliminate congestion, and increase turnover for a highly functional and efficient property.

Municipal Bylaw

Every municipal government has its bylaws including but not limited to, animal control, civil obedience (loitering, curfews in public areas like parks), property sightliness, public transit fares. These are further examples of gtechna's diverse capabilities with its law enforcement solutions.

Transportation

Transportation Demand Management is essential in today's growing metropolises and providing viable alternatives also means providing strategies to determine where to put vehicles, and how best to move people in an efficient manner. gtechna has worked with world-class transportation agencies from coast to coast including Toronto and Seattle to bring its solutions for parking, ticket fare issuance and appeals and adjudication to these agencies.

Universities and Colleges

A parking management provider for university and college campuses, gtechna experts at designing custom solutions that integrate modern, scalable software with customer infrastructure. Seamless integration with existing infrastructure makes gtechna Parking ideal for the university campus. Even high-volume enforcement is easy to manage with built-in license plate recognition.

Principal Service Commitments and System Requirements

gtechna designs its processes and procedures related to e-Citation to meet its objectives for its e-Citation solutions. Those objectives are based on the service commitments that gtechna makes to user entities, the laws and regulations that govern the provision of e-Citation solutions, and the financial, operational, and compliance requirements that gtechna has established for the solutions.

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

- Security principles within the fundamental designs of the e-Citation solutions that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

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

Components of the System

Infrastructure

Primary infrastructure used to provide gtechna's e-Citation Software Services System includes the following:

| Primary Infrastructure | | |
|-------------------------------|-----------------------------------|---|
| Hardware | Type | Purpose |
| App Servers | AWS EC2 | The in-scope application is installed on AWS EC2 virtual servers |
| Network | AWS Virtual Private Clouds (VPCs) | Cloud networking supporting all network, firewall and routing functions |

| Primary Infrastructure | | |
|-------------------------------|------------------------------|--|
| Hardware | Type | Purpose |
| Virtual Private Network (VPN) | Acceo Cisco AnyConnect VPN | Protect and restrict access to infrastructure and access to corporate network and AWS EC2 servers which is allowed by connecting to this VPN |
| Corporate network | Active Directory, Windows 10 | Third-party Acceo managed Active Directory (AD) domain which is utilized to control corporate level network access |
| Production network | AWS | Cloud hosting provider, AWS, utilized to provide cloud hosting services for in-scope production environment |
| Operating System (EC2) | CentOS Linux | Operating System used by the AWS EC2 servers |
| Databases (RDS) | PostgreSQL | RDS production databases used to support the system and store application data |
| GuardDuty | AWS | Intrusion Detection System (IDS) |
| AWS ELB | Front-end web server | Elastic Load Balancing (ELB) provides load balancing for front-end web server |
| AWS EFS | Data storage | Elastic File System (EFS) provides encrypted, redundant storage for data and stores application files |
| AWS S3 | Data storage | Provides encrypted, redundant storage for data |

Software

Primary software used to provide gtechna's e-Citation Software Services System includes the following:

| Primary Software | |
|---------------------------|--|
| Software | Purpose |
| AWS | Infrastructure |
| Linux | Operating System |
| Tomcat | Application Server |
| PostgreSQL | Database |
| e-Citation | Application Software |
| Office 365 | Third-party back-office tools for corporate SharePoint, Teams, and collaboration |
| Workday | Third-party Learning Management System (LMS) and Human Resources Information System (HRIS) |
| Zabbix | Production infrastructure monitoring |
| CloudWatch | Production infrastructure monitoring (AWS) |
| Uptime Robot | Front-end website availability monitoring |
| CrowdStrike | Third-party managed centralized workstation antivirus |
| Managed Engine MSP (Zoho) | System for service desk and gtechna support portal and change control tracking |

| Primary Software | |
|----------------------|--|
| Software | Purpose |
| Atlassian Jira | Change management, bug tracking, issue tracking |
| SVN | Change management version control software and source code repository |
| Atlassian Confluence | Internal knowledge base |
| Thycotic Secret | Password and authentication management |
| Google Authenticator | Multi-factor authentication (MFA) |
| Elastic | Application performance monitoring APM and security and vulnerability scanning |

People

gtechna is a business unit of Acceo Solutions Inc, which is a division of Harris Computer System, which is part of the Constellation Software group (CSU: TSE).

gtechna has grown into a community of 50 friendly, experienced highly trained professionals who provide the most up-to-date expertise in information technology. The group of professionals brings best practices informed by global trends in information technology to build software applications for the parking, code enforcement, and public safety markets.

Team gtechna believes in nurturing relationships first and business second in order to gain deeper insights into the needs of clients. Ensuring that staff and clients are enjoying the business process is as important as the results. Surpassing client expectations and making new friendships along the way are what make gtechna's success stories truly exceptional.

The gtechna team is structured in five main operational groups, Sales and Marketing, Professional Services, R&D, Customer Success and Finance and Administration.

Data

Main components of the e-Citation solutions are the following modules and services:

- Ticketing
- License Plate Recognition
- Permit and Visitor Management
- Business Intelligence
- Hosting

Processes, Policies and Procedures

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

Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope services. Refer to the "Subservice Organization" table below for controls managed by AWS.

Wholly occupied company office facilities are protected by access cards and all accesses are logged.

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

Logical Access

gtechna uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and supplemental 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, gtechna 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.

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

Employees and approved vendor personnel sign on to the gtechna network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords 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 change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the system from outside the gtechna network are required to use a token-based two-factor authentication system. Employees are issued tokens upon employment and must return the token during their exit interview. Vendor personnel are not permitted to access the system from outside the gtechna network.

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

Computer Operations - Backups

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

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

Computer Operations - Availability

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

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

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

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

Change Control

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

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

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

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

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Administrative access to the firewall is restricted to authorized employees.

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

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

Boundaries of the System

The scope of this report includes the e-Citation Software Services System performed at the Montreal, Quebec facilities.

This report does not include the cloud hosting services provided by AWS 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 gtechna's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of gtechna's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

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

Commitment to Competence

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

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

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

Management's Philosophy and Operating Style

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

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

- Management is briefed at least annually 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

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

gtechna'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 Resources Policies and Practices

gtechna'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 ensure the service organization operates at maximum efficiency. gtechna's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

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

Risk Assessment Process

gtechna's risk assessment process identifies and manages risks that could potentially affect gtechna'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. gtechna identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by gtechna, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

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

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of gtechna's e-Citation Software Services System; as well as the nature of the components of the system result in risks that the criteria will not be met. gtechna 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, gtechna's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of gtechna'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 gtechna, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, all hands meetings are held monthly to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead all hands 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 gtechna personnel via e-mail messages.

Specific information systems used to support gtechna's e-Citation Software 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. gtechna's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

gtechna'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 gtechna'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 gtechna'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 gtechna e-Citation Software Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS in the multiple facilities around the US.

Subservice Description of Services

AWS provides the secure hosting and staging of gtechna's production infrastructure.

Complementary Subservice Organization Controls

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

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 |
| Common Criteria / Security | CC6.4 | 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. |

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

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

COMPLEMENTARY USER ENTITY CONTROLS

gtechna'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 gtechna's services to be solely achieved by gtechna control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of gtechna'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 gtechna.
2. User entities are responsible for notifying gtechna 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 gtechna 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 gtechna services.
6. User entities are responsible for providing gtechna with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying gtechna of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security Category)

Security refers to the protection of:

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

Control Activities Specified by the Service Organization

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

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

SECTION 4

**TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND
TESTS OF CONTROLS**

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

A-LIGN ASSURANCE's examination of the controls of gtechna was limited to the Trust Services Criteria, related criteria and control activities specified by the management of gtechna and did not encompass all aspects of gtechna'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. | <p>Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.</p> <p>An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.</p> <p>Policies and procedures documented for significant processes are available on the entity's intranet.</p> <p>Prior to employment, personnel are required to complete and pass a background check.</p> | <p>Inspected the employee handbook, code of conduct, information security policies and procedures 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.</p> <p>Inspected the employee handbook and code of conduct to determine that an employee handbook and code of conduct were documented to communicate workforce conduct standards and enforcement procedures.</p> <p>Inspected the entity's intranet to determine that policies and procedures documented for significant processes were available on the entity's intranet.</p> <p>Inspected the completed background check for a sample of new hires to determine that prior to employment, personnel were required to complete and pass a background check.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 proprietary rights and confidentiality agreement upon hire. | Inspected the completed proprietary rights acknowledgement for a sample of new hires to determine that personnel were required to acknowledge the proprietary rights and confidentiality agreement upon hire. | No exceptions noted. |
| | | Personnel are required to acknowledge the employee handbook and code of conduct upon hire. | Inspected the completed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that personnel were required to acknowledge the employee handbook and code of conduct upon hire. | No exceptions noted. |
| | | Personnel are required to complete information security and awareness training upon hire as a part of training compliance. | Inspected the security awareness and training policies and procedures, the training material and program, and the training completion record for a sample of new hires to determine that personnel were required to complete information security and awareness training upon hire as a part of training compliance. | No exceptions noted. |
| | | Personnel are required to acknowledge the employee handbook on an annual basis or upon major updates to ensure user consent to changes. | Inquired of the IT Infrastructure and Security Team Lead regarding employee handbook updates and acknowledgement procedures to determine that personnel were required to acknowledge the employee handbook on an annual basis or upon major updates to ensure user consent to changes. | No exceptions noted. |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Control Environment

| CC1.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|----------|--|---|---|
| | | Performance and conduct evaluations are performed for personnel on an annual basis. | <p>Inspected the employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis or upon major updates to ensure user consent to changes.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding performance evaluation procedures to determine that performance and conduct evaluations were performed for personnel on an annual basis.</p> <p>Inspected the employee performance evaluation policies and procedures to determine that performance and conduct evaluations were performed for personnel on an annual basis.</p> <p>Inspected the completed performance review for a sample of current employees to determine that performance and conduct evaluations were scheduled to be performed for personnel on an annual basis.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |
| | | Sanction policies, which include disciplinary actions, are in place for employee misconduct. | Inspected the employee handbook and sanction policies and procedures to determine that sanction policies, which included disciplinary actions, were in place for employee misconduct. | No exceptions noted. |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Control Environment

| CC1.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|--|---|---|--|
| CC1.2 | COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | Employees are directed on how to report unethical behavior in a confidential manner. | Inspected the employee handbook and the unethical reporting and escalation policies and procedures to determine that employees were directed on how to report unethical behavior in a confidential manner. | No exceptions noted. |
| | | An anonymous hotline is in place to allow employees to report unethical behavior in a confidential manner. | Inspected the anonymous hotline number and procedures to determine that an anonymous hotline was in place to allow employees to report unethical behavior in a confidential manner. | No exceptions noted. |
| | | Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place and made available to personnel through the entity's intranet. | Inspected the information security and incident escalation policies and procedures and the entity's intranet to determine that documented escalation procedures for reporting system failures, incidents, concerns, and other complaints were in place and made available to personnel through the entity's intranet. | No exceptions noted. |
| | | Executive management defines and documents the skills and expertise needed among its members. Executive management roles and responsibilities are documented and reviewed as needed. | Inspected the job description for a sample of roles to determine that executive management defined and documented the skills and expertise needed among its members. Inspected the executive management strategy meeting presentation deck with review of roles and responsibilities to determine that executive management roles and responsibilities were documented and reviewed as needed. | No exceptions noted. No exceptions noted. |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Control Environment

| CC1.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|----------|--|--|----------------------|
| | | Executive management evaluates the skills and expertise of its members annually. | Inspected the executive management strategy meeting presentation deck with review of employee skills and expertise 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 within the environment. | Inspected the completed evaluation 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 within the environment. | Inspected the organizational chart, management meeting minutes, and internal controls matrix to determine that executive management maintained independence from those that operate the key controls within the environment. | No exceptions noted. |
| | | Executive management meets annually with operational management to assess the effectiveness and performance of internal controls within the environment. | Inspected the management meeting presentation deck to determine that executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment. | No exceptions noted. |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Control Environment

| CC1.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|---|---|---|---|
| CC1.3 | COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | <p>Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.</p> <p>A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.</p> <p>The organizational chart is updated on a real-time basis via the entity's human resources software, and updates are made to the organizational structure and lines of reporting, if necessary.</p> <p>Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.</p> <p>Executive management has established proper segregations of duties for key job functions and roles within the organization.</p> | <p>Inspected the management meeting minutes to determine that operational management assigned responsibility for and monitored the effectiveness and performance of internal controls within the environment.</p> <p>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.</p> <p>Inspected the organizational chart to determine that the organizational chart was updated on a real-time basis via the entity's human resources software, and that updates were made to the organizational structure and lines of reporting, if necessary.</p> <p>Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.</p> <p>Inspected the organizational chart, internal controls matrix, and the job description for an example job role to determine that executive management established proper segregations of duties for key job functions and roles within the organization.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Control Environment

| CC1.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|--|---|---|---|
| CC1.4 | COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | <p>Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.</p> <p>The entity is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives.</p> <p>The entity evaluates the competencies and experience of candidates prior to hiring.</p> <p>Prior to employment, personnel are required to complete and pass a background check.</p> | <p>Inspected the employee performance evaluation and training policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.</p> <p>Inspected the HR and recruitment procedures and program and the job posting for an open position to determine that the entity was responsible for attracting individuals with competencies and experience that aligned with the entity's goals and objectives.</p> <p>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.</p> <p>Inspected the completed background check for a sample of new hires to determine that prior to employment, personnel were required to complete and pass a background check.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 proprietary rights and confidentiality agreement upon hire. | Inspected the completed proprietary rights acknowledgement for a sample of new hires to determine that personnel were required to acknowledge the proprietary rights and confidentiality agreement upon hire. | No exceptions noted. |
| | | Personnel are required to acknowledge the employee handbook and code of conduct upon hire. | Inspected the completed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that personnel were required to acknowledge the employee handbook and code of conduct upon hire. | No exceptions noted. |
| | | Personnel are required to complete information security and awareness training upon hire as a part of training compliance. | Inspected the security awareness and training policies and procedures, the training material and program, and the training completion record for a sample of new hires to determine that personnel were required to complete information security and awareness training upon hire as a part of training compliance. | No exceptions noted. |
| | | Performance and conduct evaluations are performed for personnel on an annual basis. | Inquired of the IT Infrastructure and Security Team Lead regarding performance evaluation procedures 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 |
|-------|----------|--|---|---|
| | | As part of the performance evaluation process, the entity rewards its personnel for exceeding expectations as it relates to their job role and responsibilities. | <p>Inspected the employee performance evaluation policies and procedures to determine that performance and conduct evaluations were performed for personnel on an annual basis.</p> <p>Inspected the completed performance review for a sample of current employees to determine that performance and conduct evaluations were scheduled to be performed for personnel on an annual basis.</p> <p>Inspected the employee performance evaluation policies and procedures to determine that as part of the performance evaluation process, the entity rewarded its personnel for exceeding expectations as it relates to their job role and responsibilities.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |
| | | Management has created a training program for its employees. | Inspected the training program and learning platform dashboard to determine that management had created a training program for its employees. | No exceptions noted. |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Control Environment

| CC1.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|---|---|---|-----------------------------|
| | | <p>The entity provides training programs for employees, including continuing education training for continued professional development and technical skills training for technical and job role competency and development.</p> | <p>Inspected the training program and learning platform dashboard, the training tracker, and the completed training record for a sample of employees to determine that the entity provided training programs for employees, including continuing education training for continued professional development and technical skills training for technical and job role competency and development.</p> | <p>No exceptions noted.</p> |
| | | <p>Management tracks and monitors compliance training requirements.</p> | <p>Inspected the learning management system dashboard, the training policy, and the training tracker to determine that management tracked and monitored compliance training requirements.</p> | <p>No exceptions noted.</p> |
| | | <p>Sanction policies, which include disciplinary actions, are in place for employee misconduct.</p> | <p>Inspected the employee handbook and sanction policies and procedures to determine that sanction policies, which included disciplinary actions, were in place for employee misconduct.</p> | <p>No exceptions noted.</p> |
| | | <p>The entity has implemented a mentor program to develop its personnel.</p> | <p>Inspected the mentor program to determine that the entity implemented a mentor program to develop its personnel.</p> | <p>No exceptions noted.</p> |
| CC1.5 | <p>COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</p> | <p>A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.</p> | <p>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.</p> | <p>No exceptions noted.</p> |

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 |
|-------|----------|--|---|-----------------------------|
| | | <p>Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.</p> | <p>Inspected the employee performance evaluation and training policies and procedures to determine that policies and procedures were in place that outlined the performance evaluation process as well as the competency and training requirements for personnel.</p> | <p>No exceptions noted.</p> |
| | | <p>Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.</p> | <p>Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.</p> | <p>No exceptions noted.</p> |
| | | <p>Personnel are required to acknowledge the employee handbook and code of conduct upon hire.</p> | <p>Inspected the completed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that personnel were required to acknowledge the employee handbook and code of conduct upon hire.</p> | <p>No exceptions noted.</p> |
| | | <p>Personnel are required to acknowledge the employee handbook on an annual basis or upon major updates to ensure user consent to changes.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding employee handbook updates and acknowledgement procedures to determine that personnel were required to acknowledge the employee handbook on an annual basis or upon major updates to ensure user consent to changes.</p> | <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Control Environment

| CC1.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|----------|--|---|---|
| | | Performance and conduct evaluations are performed for personnel on an annual basis. | <p>Inspected the employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis or upon major updates to ensure user consent to changes.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding performance evaluation procedures to determine that performance and conduct evaluations were performed for personnel on an annual basis.</p> <p>Inspected the employee performance evaluation policies and procedures to determine that performance and conduct evaluations were performed for personnel on an annual basis.</p> <p>Inspected the completed performance review for a sample of current employees to determine that performance and conduct evaluations were scheduled to be performed for personnel on an annual basis.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |
| | | Sanction policies, which include disciplinary actions, are in place for employee misconduct. | Inspected the employee handbook and sanction policies and procedures to determine that sanction policies, which included disciplinary actions, were in place for employee misconduct. | No exceptions noted. |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Information and Communication

| CC2.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|---|--|---|---|
| CC2.1 | COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | <p>Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes are made available to personnel through the entity's intranet.</p> <p>Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.</p> <p>Network and data flow diagrams are documented and maintained by management to identify the relevant internal and external information sources of the system.</p> <p>Data that entered into the system, processed by the system, and output from the system is protected from unauthorized access.</p> | <p>Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes were made available to personnel through the entity's intranet.</p> <p>Inspected the system edit check configurations to determine that edits checks were in place to prevent incomplete or incorrect data from being entered into the system.</p> <p>Inspected the network and data flow diagrams to determine that network and data flow diagrams were documented and maintained by management to identify the relevant internal and external information sources of the system.</p> <p>Inspected the system data protection and authentication configurations, IDS configurations, firewall rules, and encryption mechanisms to determine that data entered into the system, processed by the system, and output from the system was protected from unauthorized access.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Information and Communication

| CC2.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|--|--|--|----------------------|
| CC2.2 | COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | Data and information critical to the system is assessed at least annually for completeness, accuracy, relevance, and use. | Inspected the completed data criticality assessment and the data dictionary to determine that data and information critical to the system was assessed at least annually for completeness, accuracy, relevance, and use. | No exceptions noted. |
| | | Data is retained for as long as required to perform the necessary system functionality, service, or use, or as per defined in third-party agreements. | Inspected the data retention policies and procedures to determine that data was retained for as long as required to perform the necessary system functionality, service, or use, or as per defined in third-party agreements. | No exceptions noted. |
| | | Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes are made available to personnel through the entity's intranet. | Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes were made available to personnel through the entity's intranet. | No exceptions noted. |
| | | Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet. | Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet. | No exceptions noted. |

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 |
|-------|----------|---|---|-----------------------------|
| | | <p>Policies and procedures documented for significant processes are available on the entity's intranet.</p> | <p>Inspected the entity's intranet to determine that policies and procedures documented for significant processes were available on the entity's intranet.</p> | <p>No exceptions noted.</p> |
| | | <p>Personnel are required to acknowledge the proprietary rights and confidentiality agreement upon hire.</p> | <p>Inspected the completed proprietary rights acknowledgement for a sample of new hires to determine that personnel were required to acknowledge the proprietary rights and confidentiality agreement upon hire.</p> | <p>No exceptions noted.</p> |
| | | <p>Personnel are required to acknowledge the employee handbook and code of conduct upon hire.</p> | <p>Inspected the completed employee handbook and code of conduct acknowledgement for a sample of new hires to determine that personnel were required to acknowledge the employee handbook and code of conduct upon hire.</p> | <p>No exceptions noted.</p> |
| | | <p>Management has created a training program for its employees.</p> | <p>Inspected the training program and learning platform dashboard to determine that management had created a training program for its employees.</p> | <p>No exceptions noted.</p> |
| | | <p>Personnel are required to complete information security and awareness training upon hire as a part of training compliance.</p> | <p>Inspected the security awareness and training policies and procedures, the training material and program, and the training completion record for a sample of new hires to determine that personnel were required to complete information security and awareness training upon hire as a part of training compliance.</p> | <p>No exceptions noted.</p> |

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 |
|-------|----------|---|---|---|
| | | <p>Management tracks and monitors compliance training requirements.</p> <p>Personnel are required to acknowledge the employee handbook on an annual basis or upon major updates to ensure user consent to changes.</p> <p>Executive management meets annually with operational management to discuss the entity's objectives as well as roles and responsibilities.</p> | <p>Inspected the learning management system dashboard, the training policy, and the training tracker to determine that management tracked and monitored compliance training requirements.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding employee handbook updates and acknowledgement procedures to determine that personnel were required to acknowledge the employee handbook on an annual basis or upon major updates to ensure user consent to changes.</p> <p>Inspected the employee handbook acknowledgement for a sample of current employees to determine that personnel were required to acknowledge the employee handbook on an annual basis or upon major updates to ensure user consent to changes.</p> <p>Inspected the management meeting presentation deck to determine that executive management met annually with operational management to discuss the entity's objectives as well as roles and responsibilities.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|--|---|---|
| | | <p>Employees are directed on how to report unethical behavior in a confidential manner.</p> <p>An anonymous hotline is in place to allow employees to report unethical behavior in a confidential manner.</p> <p>Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place and made available to personnel through the entity's intranet.</p> | <p>Inspected the employee handbook and the unethical reporting and escalation policies and procedures to determine that employees were directed on how to report unethical behavior in a confidential manner.</p> <p>Inspected the anonymous hotline number and procedures to determine that an anonymous hotline was in place to allow employees to report unethical behavior in a confidential manner.</p> <p>Inspected the information security and incident escalation policies and procedures and the entity's intranet to determine that documented escalation procedures for reporting system failures, incidents, concerns, and other complaints were in place and made available to personnel through the entity's intranet.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Information and Communication

| CC2.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--------------|---|--|---|---|
| CC2.3 | COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | <p>Agreements are in place with third parties to:</p> <ul style="list-style-type: none"> • Delineate the boundaries of the system and describe relevant system components • Communicate the system commitments and requirements • Outline and communicate the terms, conditions, and responsibilities <p>The entity's contractor agreement outlines and communicates the terms, conditions, and responsibilities of external users.</p> <p>Customer commitments, requirements, and responsibilities are outlined and communicated through service agreements.</p> | <p>Inspected the third-party agreement templates and the executed agreement for a sample of third parties to determine that agreements were in place with third parties to:</p> <ul style="list-style-type: none"> • Delineate the boundaries of the system and describe relevant system components • Communicate the system commitments and requirements • Outline and communicate the terms, conditions, and responsibilities <p>Inspected the contractor agreement template to determine that the entity's contractor agreement outlined and communicated the terms, conditions, and responsibilities of external users.</p> <p>Inspected the customer service agreement templates and the executed agreement for a sample of customers to determine that customer commitments, requirements, and responsibilities were outlined and communicated through service agreements.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|---|---|---|
| | | <p>Changes to commitments, requirements and responsibilities are communicated to third parties and customers via updated agreements, mass notifications, e-mail, and the contract management team.</p> <p>Documented escalation procedures for reporting failures, incidents, concerns, and other complaints are in place and shared with external parties.</p> | <p>Inspected the entity's procedures regarding third party and customer communication and changes to commitments and an example change in commitment communication to determine that changes to commitments, requirements and responsibilities were communicated to third parties and customers via updated agreements, mass notifications, e-mail, and the contract management team.</p> <p>Inspected the incident management and escalation policies and procedures, the support services agreement, and the entity's support portal to determine that documented escalation procedures for reporting failures, incidents, concerns, and other complaints were in place and shared with external parties.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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. | <p>The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.</p> <p>Executive management has documented objectives that are specific, measurable, attainable, relevant, and time-bound (SMART).</p> <p>Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.</p> <p>Executive management has established key performance indicators for operational and internal controls effectiveness, including the acceptable level of control operation and failure.</p> | <p>Inspected the organizational objectives and strategies to determine that the entity established organizational strategies and objectives that were used to determine entity structure and performance metrics.</p> <p>Inspected the organizational objectives and strategies to determine that executive management had documented objectives that were SMART.</p> <p>Inspected the risk assessment 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.</p> <p>Inspected the 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.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Risk Assessment

| CC3.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|----------|--|---|----------------------|
| | | Key performance indicators of both the business performance and employee performance are developed in alignment with entity objectives and strategies. | Inspected the key performance indicators, organizational objectives and strategies, and the employee performance evaluation policies and procedures to determine that key performance indicators of both the business performance and employee performance were developed in alignment with entity objectives and strategies. | No exceptions noted. |
| | | Business plans and budgets align with the entity's strategies and objectives. | Inspected the entity's business plans, budget and organizational objectives and strategies to determine that business plans and budgets aligned with the entity's strategies and objectives. | No exceptions noted. |
| | | Entity strategies, objectives and budgets are assessed on at least an annual basis. | Inspected the executive management meeting presentation deck including review of business plans, budget, objectives, and strategies to determine that entity strategies, objectives and budgets were assessed on at least an annual basis. | No exceptions noted. |
| | | The entity's internal controls environment takes into consideration affecting laws, regulations, standards, and legislatures. | Inspected the entity's policies and procedures related to the relevant requirements and the current requirements registry to determine that the entity's internal controls environment took into consideration affecting laws, regulations, standards, and legislatures. | No exceptions noted. |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Risk Assessment

| CC3.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|---|---|--|---|
| 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. | <p>Applicable law, regulation, standard and legislature requirements are identified and integrated into the entity's strategies and objectives.</p> <p>Documented policies and procedures are in place to guide personnel when performing a risk assessment.</p> <p>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.</p> | <p>Inspected the entity's objectives and strategies, policies and procedures related to the relevant requirements, the current requirements registry, and the completed risk assessment to determine that applicable law, regulation, standard and legislature requirements were identified and integrated into the entity's strategies and objectives.</p> <p>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.</p> <p>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.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|---|---|---|
| | | <p>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.</p> <p>Identified risks are rated using a risk analysis and evaluation process.</p> <p>Risks identified as a part of the risk assessment process are addressed using one of the following strategies:</p> <ul style="list-style-type: none"> • Avoid the risk • Accept the risk • Reduce the risk <p>Management develops risk mitigation strategies to address risks identified during the risk assessment process.</p> | <p>Inspected the risk assessment policies and procedures and 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.</p> <p>Inspected the risk assessment policies and procedures and the completed risk assessment to determine that identified risks were rated using a risk analysis and evaluation process.</p> <p>Inspected the risk assessment policies and procedures and the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies:</p> <ul style="list-style-type: none"> • Avoid the risk • Accept the risk • Reduce the risk <p>Inspected the risk assessment, management, and mitigation 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.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|--------------|--|---|--|----------------------|
| CC3.3 | COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. | Management identifies and assesses the types of fraud that could impact their business and operations. | Inspected the completed fraud and risk assessment to determine that management identified and assessed the types of fraud that could impact their business and operations. | No exceptions noted. |
| | | As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT. | Inspected the completed fraud and risk 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. |
| | | Risks identified as a part of the risk assessment process are addressed using one of the following strategies: <ul style="list-style-type: none"> • Avoid the risk • Accept the risk • Reduce the risk | Inspected the risk assessment policies and procedures and the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: <ul style="list-style-type: none"> • Avoid the risk • Accept the risk • Reduce the risk | No exceptions noted. |
| 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 policies and procedures 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. |

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 |
|-------|----------|---|---|---|
| | | <p>Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.</p> <p>Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.</p> | <p>Inspected the risk assessment 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.</p> <p>Inspected the risk assessment 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.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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. | <p>Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs, and unusual system activity.</p> <p>The monitoring software is configured to alert appropriate IT personnel when thresholds have been exceeded.</p> <p>An IDS is utilized to analyze network events and report possible or actual network security breaches.</p> <p>The IDS is configured to notify appropriate IT personnel upon intrusion detection.</p> | <p>Inspected the monitoring system and alert 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.</p> <p>Inspected the monitoring system notification configurations, dashboards, log reports, and a sample of monitoring alert notifications to determine that the monitoring software was configured to alert appropriate IT personnel when thresholds had been exceeded.</p> <p>Inspected the IDS configurations and system dashboard to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.</p> <p>Inspected the IDS alert notification configurations and an example IDS alert notification to determine that the IDS is configured to notify appropriate IT personnel upon intrusion detection.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|---|--|-----------------------------|
| | | <p>Management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses on at least an annual basis.</p> | <p>Inspected the management meeting minutes and the completed internal controls matrix to determine that management reviewed the controls implemented within the environment for operational effectiveness and identified potential control gaps and weaknesses on at least an annual basis.</p> | <p>No exceptions noted.</p> |
| | | <p>Logical access reviews are performed on at least an annual basis.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding logical user access reviews to determine that logical access reviews were performed on at least an annual basis.</p> | <p>No exceptions noted.</p> |
| | | <p>Data backup restoration tests are performed on an annual basis.</p> | <p>Inspected the completed logical user access reviews to determine that logical access reviews were performed on at least an annual basis.</p> | <p>No exceptions noted.</p> |
| | | <p>Data backup restoration tests are performed on an annual basis.</p> | <p>Inspected the completed backup restoration test to determine that data backup restoration tests were performed on an annual basis.</p> | <p>No exceptions noted.</p> |
| | | <p>Vulnerability scans are performed at least semi-annually on the environment to identify control gaps and vulnerabilities.</p> | <p>Inspected the completed vulnerability scan report and results to determine that vulnerability scans were performed at least semi-annually on the environment to identify control gaps and vulnerabilities.</p> | <p>No exceptions noted.</p> |

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 |
|-------|----------|---|---|---|
| | | <p>A third party performs a penetration test annually to identify and exploit vulnerabilities identified within the environment.</p> <p>Performance and conduct evaluations are performed for personnel on an annual basis.</p> | <p>Inspected the completed third-party penetration test report and results to determine that a third party performed a penetration test annually to identify and exploit vulnerabilities identified within the environment.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding performance evaluation procedures to determine that performance and conduct evaluations were performed for personnel on an annual basis.</p> <p>Inspected the employee performance evaluation policies and procedures to determine that performance and conduct evaluations were performed for personnel on an annual basis.</p> <p>Inspected the completed performance review for a sample of current employees to determine that performance and conduct evaluations were scheduled to be performed for personnel on an annual basis.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Monitoring Activities

| CC4.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|--|---|---|--|
| CC4.2 | COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. | Vendor systems are subject to review as part of the vendor risk management process. Attestation reports are obtained and evaluated when available for high-risk or critical vendors. | Inspected the vendor risk assessment and management policies and procedures and the completed third-party risk assessment including critical vendor attestation report review to determine that vendor systems were subject to review as part of the vendor risk management process, and that, attestation reports were obtained and evaluated when available for high-risk or critical vendors. | 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 risk assessment policies and procedures and 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. |
| | | Senior management assesses the results of the compliance, control and risk assessments performed on the environment. Vulnerability scans are performed at least semi-annually on the environment to identify control gaps and vulnerabilities. | Inspected the management meeting minutes to determine that senior management assessed the results of the compliance, control and risk assessments performed on the environment. Inspected the completed vulnerability scan report and results to determine that vulnerability scans were performed at least semi-annually on the environment to identify control gaps and vulnerabilities. | No exceptions noted. 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 |
|-------|----------|---|---|---|
| | | <p>A third party performs a penetration test annually to identify and exploit vulnerabilities identified within the environment.</p> <p>Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions.</p> | <p>Inspected the completed third-party penetration test report and results to determine that a third party performed a penetration test annually to identify and exploit vulnerabilities identified within the environment.</p> <p>Inspected the various completed assessments performed on the environment to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions.</p> <p>Inspected the supporting remediation ticket for a sample of deviations to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>Testing of the control activity disclosed that no critical or high risk deviations were identified during the review period.</p> |

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 |
|-------|----------|--|--|--|
| | | <p>Vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments are documented, investigated, and addressed.</p> | <p>Inspected the supporting remediation ticket and report for a sample of vulnerabilities identified from a penetration test or vulnerability scan report to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were communicated to those parties responsible for taking corrective actions.</p> <p>Inspected the various completed assessments performed on the environment to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were documented, investigated and addressed.</p> <p>Inspected the supporting remediation ticket for a sample of deviations to determine that vulnerabilities, deviations, and control gaps identified from the compliance, control and risk assessments were documented, investigated and addressed.</p> | <p>Testing of the control activity disclosed that no critical or high risk vulnerabilities were identified from a penetration test or vulnerability scan during the review period.</p> <p>No exceptions noted.</p> <p>Testing of the control activity disclosed that no critical or high risk deviations were identified during the review period.</p> |

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 |
|-------|----------|---|--|--|
| | | <p>Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed in a timely manner.</p> | <p>Inspected the supporting remediation ticket and report for a sample of vulnerabilities identified from a penetration test or vulnerability scan report to determine that vulnerabilities, deviations, and control gaps from the compliance, control and risk assessments were documented, investigated, and addressed.</p> <p>Inspected the management meeting minutes and presentation decks and the incident management tracking report dashboard to determine that management tracked whether vulnerabilities, deviations, and control gaps identified as part of the evaluations performed were addressed in a timely manner.</p> | <p>Testing of the control activity disclosed that no critical or high risk vulnerabilities were identified from a penetration test or vulnerability scan during the review period.</p> <p>No exceptions noted.</p> |

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 | <p>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.</p> | <p>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.</p> <p>Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.</p> | <p>Inspected the risk assessment policies and procedures and 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.</p> <p>Inspected the various completed assessments performed on the environment 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.</p> <p>Inspected the supporting remediation ticket for a sample of deviations, 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.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>Testing of the control activity disclosed that no critical or high risk deviations were identified during the review period.</p> |

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 |
|-------|----------|---|--|--|
| | | <p>Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.</p> <p>Management has relevant controls in place for key business, operational and technology processes.</p> <p>Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.</p> | <p>Inspected the supporting remediation ticket and report for a sample of vulnerabilities identified from a penetration test to determine that controls within the environment were modified and implemented to mitigate vulnerabilities, deviations, and control gaps identified as part of the various evaluations performed.</p> <p>Inspected the organizational chart and 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.</p> <p>Inspected the internal controls matrix to determine that management relevant controls in place for key business, operational and technology processes.</p> <p>Inspected the internal controls matrix to determine that management incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.</p> | <p>Testing of the control activity disclosed that no critical or high risk vulnerabilities were identified from a penetration test or vulnerability scan during the review period.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Control Activities

| CC5.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|--|--|--|----------------------|
| CC5.2 | COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. | Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. | Inspected the risk assessment, management, and mitigation policies and procedures and the completed risk assessment to determine that management developed risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process. | No exceptions noted. |
| | | 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. |
| | | Data backup restoration tests are performed on an annual basis. | Inspected the completed backup restoration test to determine that data backup restoration tests were performed on an annual basis. | No exceptions noted. |
| | | Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes are made available to personnel through the entity's intranet. | Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes were made available to personnel through the entity's intranet. | 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 |
|-------|---|--|---|---|
| | | <p>Management has established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.</p> <p>The internal controls implemented around the entity's technology infrastructure include, but are not limited to:</p> <ul style="list-style-type: none"> • Restricting access rights to authorized users • Limiting services to what is required for business operations • Authentication of access • Protecting the entity's assets from external threats | <p>Inspected the completed risk assessment and the internal controls matrix to determine that management established controls around the entity's technology infrastructure to address the risks of incomplete, inaccurate, and unavailable technology processing.</p> <p>Inspected the completed risk assessment and the internal controls matrix to determine that the internal controls implemented around the entity's technology infrastructure included, but were not limited to:</p> <ul style="list-style-type: none"> • Restricting access rights to authorized users • Limiting services to what was required for business operations • Authentication of access • Protecting the entity's assets from external threats | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |
| CC5.3 | <p>COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.</p> | <p>Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes are made available to personnel through the entity's intranet.</p> | <p>Inspected the organizational and information security policies and procedures and the entity's intranet to determine that organizational and information security policies and procedures were documented for supporting the functioning of controls and processes were made available to personnel through the entity's intranet.</p> | <p>No exceptions noted.</p> |

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 |
|-------|----------|---|---|---|
| | | <p>Management has implemented controls that are built into the organizational and information security policies and procedures.</p> <p>Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's intranet.</p> <p>Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.</p> | <p>Inspected the organizational and information security policies and procedures and the internal controls matrix to determine that management implemented controls that were built into the organizational and information security policies and procedures.</p> <p>Inspected the job description for a sample of job roles and the entity's intranet to determine that roles and responsibilities were defined in written job descriptions and communicated to personnel through the entity's intranet.</p> <p>Inspected the organizational chart and 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.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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. | <p>Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.</p> <p>An inventory of system assets and components is in place to classify and manage information assets and inventory components.</p> <p>Logical access to systems is approved and granted to an employee as a component of the hiring process.</p> <p>Logical access to systems is revoked as a component of the termination process.</p> | <p>Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.</p> <p>Inspected the inventory listing of system assets and components to determine that an inventory of system assets and components was in place to classify and manage information assets and inventory components.</p> <p>Inspected the hiring and access control policies and procedures and the onboarding access e-mail and 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.</p> <p>Inquired of the System Administrator regarding termination procedures to determine that logical access to systems was revoked as a component of the termination process.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 reviews are performed on at least an annual basis. | <p>Inspected the termination and access control policies and procedures, system user access listings, and the deactivation e-mail and access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding logical user access reviews to determine that logical access reviews were performed on at least an annual basis.</p> <p>Inspected the completed logical user access reviews to determine that logical access reviews were performed on at least an annual basis.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |
| | | Privileged access to sensitive resources is restricted to authorized and appropriate personnel. | <p>Inquired of the IT Infrastructure and Security Team Lead regarding privileged access to sensitive resources to determine that privileged access to sensitive resources was restricted to authorized and appropriate personnel.</p> <p>Inspected the listings of privileged users with system access to sensitive resources to determine that privileged access to sensitive resources was restricted to authorized and appropriate personnel.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|---|---|---|---|
| | | Audit logging settings are in place for critical information system activity and events and logs are maintained and reviewed as needed. | <p>Inquired of the IT Infrastructure and Security Team Lead regarding critical system audit logging to determine that audit logging settings were in place for critical information system activity and events, and that, logs were maintained and reviewed as needed.</p> <p>Inspected the system audit logging configurations and an example event audit log extract to determine that audit logging settings were in place for critical information system activity and events, and that, logs were maintained and reviewed as needed.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |
| | Corporate Network (Active Directory) | | | |
| | | Network user access is restricted via role-based security privileges defined within the access control system. | <p>Inquired of the IT Infrastructure and Security Team Lead regarding corporate network access control and 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.</p> <p>Inspected the network user listing to determine that network user access was restricted via role-based security privileges defined within the access control system.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|--|---|---|
| | | <p>Networks are configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> • Password history • Password age • Password length • Complexity <p>Network account lockout settings are in place that include:</p> <ul style="list-style-type: none"> • Account lockout duration • Account lockout threshold • Account lockout counter reset <p>Network devices are configured to log events and access attempts to ensure that system activity can be traced to a specific user and that necessary data is available in the system logs to support audit and other related business functions.</p> | <p>Inspected the network password policy and authentication configurations to determine that networks were configured to enforce password requirements that included:</p> <ul style="list-style-type: none"> • Password history • Password age • Password length • Complexity <p>Inspected the network account lockout settings to determine that network account lockout settings were in place that included:</p> <ul style="list-style-type: none"> • Account lockout duration • Account lockout threshold • Account lockout counter reset <p>Inspected the network audit and event logging configurations and an example audit log extract to determine that network devices were configured to log events and access attempts to ensure that system activity could be traced to a specific user and that necessary data was available in the system logs to support audit and other related business functions.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|---------------------------------|---|--|---|
| | | <p>Network audit logging settings are in place for system events and sign-in activity and logs are maintained, monitored, and reviewed as needed.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding corporate network audit and event logging to determine that network audit logging settings were in place for system events and sign-in activity and that logs were maintained, monitored, and reviewed as needed.</p> <p>Inspected the network audit and event logging configurations and an example audit log extract to determine that network audit logging settings were in place for system events and sign-in activity and that logs were maintained, monitored, and reviewed as needed.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |
| | Production Network (AWS) | | | |
| | | <p>AWS network user access is restricted via role-based security privileges defined within the access control system.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding AWS production network access control to determine that AWS network user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inspected the AWS user listing and access rights to determine that AWS network user access was restricted via role-based security privileges defined within the access control system.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|---|--|---|
| | | <p>AWS administrative access is restricted to limited user accounts accessible by authorized and appropriate personnel.</p> <p>AWS root-level access is limited and restricted. Administrator authentication requires root user e-mail address, unique strong passwords, and MFA mobile code.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding AWS administrative access to determine that AWS administrative access was restricted to limited user accounts accessible by authorized and appropriate personnel.</p> <p>Inspected the AWS administrator listing and access rights to determine that AWS administrative access was restricted to limited user accounts accessible by authorized and appropriate personnel.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding AWS root-level authentication to the AWS production network to determine that AWS root-level access was limited and restricted, and that, administrator authentication required root user e-mail address, unique strong passwords, and MFA mobile code.</p> <p>Observed an admin user login to the root account of the production network to determine that AWS root-level access was limited and restricted, and that, administrator authentication required root user e-mail address, unique strong passwords, and MFA mobile code.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|--|--|---|
| | | <p>AWS IAM users are authenticated via individually assigned user accounts, passwords, and MFA.</p> <p>AWS is configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> • Password history • Password age • Password length • Complexity | <p>Inspected the production authentication management and configurations to determine that AWS root-level access was limited and restricted, and that, administrator authentication required root user e-mail address, unique strong passwords, and MFA mobile code.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding AWS authentication to determine that AWS IAM users were authenticated via individually assigned user accounts, passwords, and MFA.</p> <p>Observed an admin user login to AWS IAM to determine that AWS IAM users were authenticated via individually assigned user accounts, passwords, and MFA.</p> <p>Inspected the AWS user listing and password configurations to determine that AWS IAM users were authenticated via individually assigned user accounts, passwords, and MFA.</p> <p>Inspected the AWS password policy to determine that AWS was configured to enforce password requirements that included:</p> <ul style="list-style-type: none"> • Password history • Password age • Password length • Complexity | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|---|----------|--|---|---|
| | | <p>AWS audit logging settings are in place for usage and activity and logs are maintained and reviewed as needed.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding audit logging to determine that AWS audit logging settings were in place for usage and activity and that logs were maintained and reviewed as needed.</p> <p>Inspected the audit logging configurations and an example audit log extract to determine that AWS audit logging settings were in place for usage and activity and that logs were maintained and reviewed as needed.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |
| Operating System (Amazon EC2 - CentOS Linux) | | | | |
| | | <p>Operating system user access is restricted via role-based security privileges defined within the access control system.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding production access control and the operating system authentication procedures to determine that operating system user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|--|--|---|
| | | <p>Operating system administrative access is restricted to user accounts accessible by authorized and appropriate personnel.</p> <p>Operating system users are authenticated via an admin account, Secure Shell (SSH) public key and MFA token verification.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding operating system administrative access to determine that operating system administrative access was restricted to user accounts accessible by authorized and appropriate personnel.</p> <p>Inspected the operating system administrator listing and access rights to determine that operating system administrative access was restricted to user accounts accessible by authorized and appropriate personnel.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding production access control and the operating system authentication procedures to determine that operating system users were authenticated via an admin account, SSH public key and MFA token verification.</p> <p>Observed an admin user authenticate to the operating system to determine that operating system users were authenticated via an admin account, SSH public key and MFA token verification.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|--|---|---|
| | | <p>Operating systems are configured to enforce SSH key authentication and password requirements that include:</p> <ul style="list-style-type: none"> • Verification code • Strict Mode • Password Days (Max) • Password Day (Min) • Password Minimum Length • Password Warning Age <p>Operating system account lockout settings are in place that include maximum authentication attempts and maximum sessions.</p> <p>Operating system audit logging settings are in place to record system authentication events and logs are maintained and reviewed as needed.</p> | <p>Inspected the operating system authentication configurations to determine that operating systems were configured to enforce SSH key authentication and password requirements that included:</p> <ul style="list-style-type: none"> • Verification code • Strict Mode • Password Days (Max) • Password Day (Min) • Password Minimum Length • Password Warning Age <p>Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included maximum authentication attempts and maximum sessions.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding operating system audit logging to determine that operating system audit logging settings were in place to record system authentication events and logs were maintained and reviewed as needed.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 operating system audit logging configurations and an example audit log extract to determine that operating system audit logging settings were in place to record system authentication events and logs were maintained and reviewed as needed. | No exceptions noted. |
| | Production Databases (Amazon RDS - PostgreSQL) | | | |
| | | Database user access is restricted via role-based security privileges defined within the access control system. | Inquired of the IT Infrastructure and Security Team Lead regarding production network access control and the database authentication procedures to determine that database user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | | Database administrative access is restricted to user accounts accessible by authorized and appropriate personnel. | Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system. Inquired of the IT Infrastructure and Security Team Lead regarding database administrative access to determine that database administrative access was restricted to user accounts accessible by authorized and appropriate personnel. | No exceptions noted. 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 |
|-------|----------|---|--|---|
| | | <p>Database access is restricted and secure with multiple levels of authentication policies. Databases are configured to enforce password and authentication requirements that include the following:</p> <ul style="list-style-type: none"> • Network authentication • O/S authentication • Specific Internet Protocol (IP) address • Secret key • MFA Token • Password length of 30 characters • Complexity including uppercase, lowercase, digits, minus, underline, special characters | <p>Inspected the database administrator listing to determine that database administrative access was restricted to user accounts accessible by authorized and appropriate personnel.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding database administrative access and authentication procedures to determine that database access was restricted and secured with multiple levels of authentication policies, and that, databases were configured to enforce password and authentication requirements that included the following:</p> <ul style="list-style-type: none"> • Network authentication • O/S authentication • Specific IP address • Secret key • MFA Token • Password length of 30 characters • Complexity including uppercase, lowercase, digits, minus, underline, special characters | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|--|---|---|---|
| | | <p>Database audit logging settings are in place for system activity and events, including logins, password failure, usage, and activity, and logs are maintained and reviewed as needed.</p> <p>Data is classified and structured in a consistent manner.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding database audit logs to determine that database audit logging settings were in place for system activity and events, including logins, password failure, usage, and activity, and that logs were maintained and reviewed as needed.</p> <p>Inspected the database audit logging configurations and an example audit log extract to determine that database audit logging settings were in place for system activity and events, including logins, password failure, usage, and activity, and that logs were maintained and reviewed as needed.</p> <p>Inspected the database schema to determine that data was classified and structured in a consistent manner.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |
| | Application (Gtechna e-Citation Software) | | | |
| | | <p>Application user access is restricted via role-based security privileges defined within the access control system.</p> | <p>Inspected the application user listing, user groups, and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system.</p> | <p>No exceptions noted.</p> |

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 |
|-------|----------|---|---|----------------------|
| | | <p>Application administrative access is restricted to user accounts accessible by authorized and appropriate personnel.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding application administrative access to determine that application administrative access was restricted to user accounts accessible by authorized and appropriate personnel.</p> | No exceptions noted. |
| | | | <p>Inspected the application administrative listing and access rights to determine that application administrative access was restricted to user accounts accessible by authorized and appropriate personnel.</p> | No exceptions noted. |
| | | <p>Application users are authenticated via user accounts, passwords, and MFA.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding application access control and authentication to determine that application users were authenticated via user accounts, passwords, and MFA.</p> | No exceptions noted. |
| | | | <p>Observed a user login to the application to determine that application users were authenticated via user accounts, passwords, and MFA.</p> | No exceptions noted. |
| | | | <p>Inspected the application password and authentication configurations to determine that application users were authenticated via user accounts, passwords, and MFA.</p> | 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 |
|-------|----------|--|--|---|
| | | <p>The application is configured with password parameters that include:</p> <ul style="list-style-type: none"> • Password case sensitivity • Password encryption • Password history • Password age (days before expiration) • Password minimum length • Password maximum length • Complexity <p>Application account lockout settings are in place that include:</p> <ul style="list-style-type: none"> • Invalid login threshold <p>Application audit logging settings are in place for system events and activity and logs are maintained and reviewed as needed.</p> | <p>Inspected the application password parameters and the password and authentication configurations to determine that application was configured with password parameters that included:</p> <ul style="list-style-type: none"> • Password case sensitivity • Password encryption • Password history • Password age (days before expiration) • Password minimum length • Password maximum length • Complexity <p>Inspected the application account lockout configurations to determine that application account lockout settings were in place that included:</p> <ul style="list-style-type: none"> • Invalid login threshold <p>Inquired of the IT Infrastructure and Security Team Lead regarding application audit logs to determine that application audit logging settings were in place for system events and activity and logs were maintained and reviewed as needed.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Logical and Physical Access Controls

| CC6.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|----------|--|---|---|
| | | | Inspected the application audit logging configurations and an example audit log extract to determine application audit logging settings were in place for system events and activity and logs were maintained and reviewed as needed. | No exceptions noted. |
| Remote Access and VPN (Cisco AnyConnect) | | | | |
| | | <p>VPN user access is restricted via role-based security privileges defined within the access control system.</p> <p>The ability to administer VPN access is restricted to user accounts accessible by authorized personnel.</p> <p>Remote connectivity users are authenticated via an authorized user account, password, and MFA token before establishing a VPN session.</p> | <p>Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding VPN administrative access to determine that the ability to administer VPN access was restricted to user accounts accessible by authorized personnel.</p> <p>Inspected the VPN administrator listing to determine that the ability to administer VPN access was restricted to user accounts accessible by authorized personnel.</p> <p>Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account, password, and MFA token before establishing a VPN session.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|--|---|---|
| | | <p>VPN audit logging is enabled to provide event history for VPN activity and logs are maintained and reviewed as needed.</p> <p>AWS load balancers are utilized to proxy traffic from the internet to internal IP addresses and for front load protection.</p> <p>Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding VPN audit logging to determine that VPN audit logging was enabled to provide event history for VPN activity and logs were maintained and reviewed as needed.</p> <p>Inspected the VPN logging configurations and an example event log extract to determine that VPN audit logging was enabled to provide event history for VPN activity and logs were maintained and reviewed as needed.</p> <p>Inspected the encryption configurations and load balancers to determine that AWS load balancers were utilized to proxy traffic from the internet to internal IP addresses and for front load protection.</p> <p>Inspected the encryption configurations for data in transit and verified digital certification to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|---|---|-----------------------------|
| | | <p>Transmission of data and digital output beyond the boundary of the system is secure through the use of encryption technologies and mechanisms.</p> | <p>Inspected the encryption policies and procedures, the encryption configurations, and the digital encryption certificates to determine that transmission of data and digital output beyond the boundary of the system was secure through the use of encryption technologies and mechanisms.</p> | <p>No exceptions noted.</p> |
| | | <p>Critical data is stored in encrypted format using industry-standard Advanced Encryption Standard (AES)-256 encryption algorithm.</p> | <p>Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using industry-standard AES-256 encryption algorithm.</p> | <p>No exceptions noted.</p> |
| | | <p>A demilitarized zone (DMZ) is in place to isolate outside access and data from the entity's environment.</p> | <p>Inspected the DMZ configurations to determine a DMZ was in place to isolate outside access and data from the entity's environment.</p> | <p>No exceptions noted.</p> |
| | | <p>Encryption keys are protected during generation, storage, use, and destruction.</p> | <p>Inspected the encryption policies and procedures, the password manager system and stored password encryption configurations to determine that encryption keys were required to be protected during generation, storage, use, and destruction.</p> | <p>No exceptions noted.</p> |
| | | <p>Stored passwords are encrypted with sha-256.</p> | <p>Inspected the password manager system and stored password encryption configurations to determine that stored passwords were encrypted with sha-256.</p> | <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Logical and Physical Access Controls

| CC6.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|---|---|--|----------------------|
| CC6.2 | Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. | The entity restricts access to its environment using the following mechanisms: <ul style="list-style-type: none"> • Classifying data • Port restrictions • Access protocol restrictions • User identification • Digital certifications | Inspected the data classification policies and procedures, listings of users with access to sensitive resources, firewall rulesets and digital certificates to determine that the entity restricted access to its environment using the following mechanisms: <ul style="list-style-type: none"> • Classifying data • Port restrictions • Access protocol restrictions • User identification • Digital certifications | No exceptions noted. |
| | | Data backup restoration tests are performed on an annual basis. | Inspected the completed backup restoration test to determine that data 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 information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring. | No exceptions noted. |
| | | Logical access to systems is approved and granted to an employee as a component of the hiring process. | Inspected the hiring and access control policies and procedures and the onboarding access e-mail and 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 as a component of the termination process. | Inquired of the System Administrator regarding termination procedures to determine that logical access to systems was revoked as a component of the termination process. | No exceptions noted. |
| | | | Inspected the termination and access control policies and procedures, system user access listings, and the deactivation e-mail and access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process. | No exceptions noted. |
| | | Logical access reviews are performed on at least an annual basis. | Inquired of the IT Infrastructure and Security Team Lead regarding logical user access reviews to determine that logical access reviews were performed on at least an annual basis. | No exceptions noted. |
| | | | Inspected the completed logical user access reviews to determine that logical access reviews were performed on at least an annual basis. | No exceptions noted. |
| | | Privileged access to sensitive resources is restricted to authorized and appropriate personnel. | Inquired of the IT Infrastructure and Security Team Lead regarding privileged access to sensitive resources to determine that privileged access to sensitive resources was restricted to authorized and appropriate 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. | <p>Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.</p> <p>Logical access to systems is approved and granted to an employee as a component of the hiring process.</p> <p>Logical access to systems is revoked as a component of the termination process.</p> | <p>Inspected the listings of privileged users with system access to sensitive resources to determine that privileged access to sensitive resources was restricted to authorized and appropriate personnel.</p> <p>Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.</p> <p>Inspected the hiring and access control policies and procedures and the onboarding access e-mail and 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.</p> <p>Inquired of the System Administrator regarding termination procedures to determine that logical access to systems was revoked as a component of the termination process.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 reviews are performed on at least an annual basis. | <p>Inspected the termination and access control policies and procedures, system user access listings, and the deactivation e-mail and access revocation ticket for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding logical user access reviews to determine that logical access reviews were performed on at least an annual basis.</p> <p>Inspected the completed logical user access reviews to determine that logical access reviews were performed on at least an annual basis.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |
| | | Privileged access to sensitive resources is restricted to authorized and appropriate personnel. | <p>Inquired of the IT Infrastructure and Security Team Lead regarding privileged access to sensitive resources to determine that privileged access to sensitive resources was restricted to authorized and appropriate personnel.</p> <p>Inspected the listings of privileged users with system access to sensitive resources to determine that privileged access to sensitive resources was restricted to authorized and appropriate personnel.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

| 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 |
| | Corporate Network (Active Directory) | | | |
| | | Network user access is restricted via role-based security privileges defined within the access control system. | Inspected the network user listing to determine that network user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | Production Network (AWS) | | | |
| | | AWS network user access is restricted via role-based security privileges defined within the access control system. | Inspected the AWS user listing and access rights to determine that AWS network user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | Operating System (Amazon EC2 - CentOS Linux) | | | |
| | | Operating system user access is restricted via role-based security privileges defined within the access control system. | Inspected the operating system user listing and access rights to determine that operating system user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | Database (Amazon RDS - PostgreSQL) | | | |
| | | Database user access is restricted via role-based security privileges defined within the access control system. | Inspected the database user listing and access rights to determine that database user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|--|---|--|---|
| Logical and Physical Access Controls | | | | |
| CC6.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
| | Application (Gtechna e-Citation Software) | | | |
| | | Application user access is restricted via role-based security privileges defined within the access control system. | Inspected the application user listing and access rights to determine that application user access was restricted via role-based security privileges defined within the access control system. | No exceptions noted. |
| | Remote Access and VPN (Cisco AnyConnect) | | | |
| 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. | VPN user access is restricted via role-based security privileges defined within the access control system. This criterion is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization. | Inspected the VPN user listing to determine that VPN user access was restricted via role-based security privileges defined within the access control system. Not applicable. | No exceptions noted. Not applicable. |
| CC6.5 | The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. | Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction. | Inspected the data disposal and destruction policies and procedures to determine policies and procedures were in place to guide personnel in data, hardware and software disposal and destruction. | No exceptions noted. |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Logical and Physical Access Controls

| CC6.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|----------|--|--|---|
| | | <p>Hardware and data that is no longer required for business purposes is purged, destroyed, and rendered unreadable.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding hardware and data disposal and destruction procedures to determine that hardware and data that was no longer required for business purposes was purged, destroyed, and rendered unreadable.</p> <p>Inspected the data disposal and destruction policies and procedures to determine that hardware and data that was no longer required for business purposes was purged, destroyed, and rendered unreadable.</p> <p>Inspected the certificate of destruction and invoice for a sample of hardware and data disposals to determine that hardware and data that was no longer required for business purposes was purged, destroyed, and rendered unreadable.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |
| | | <p>The entity purges data stored on physical assets that are no longer required for business purposes.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding destruction procedures to determine that the entity purged data stored on physical assets that were no longer required for business purposes.</p> | <p>No exceptions noted.</p> |

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 |
|-------|---|---|---|---|
| CC6.6 | The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | <p>Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.</p> <p>Network address translation (NAT) functionality is utilized to manage internal IP addresses.</p> <p>Remote connectivity users are authenticated via an authorized user account, password, and MFA token before establishing a VPN session.</p> <p>An IDS is utilized to analyze network events and report possible or actual network security breaches.</p> | <p>Inspected the certificate of destruction and invoice for a sample of purged physical assets to determine that the entity purged data stored on physical assets that were no longer required for business purposes.</p> <p>Inspected the information security policies and procedures to determine that documented policies and procedures were in place regarding system settings, authentication, access, and security monitoring.</p> <p>Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.</p> <p>Inspected the VPN authentication configurations to determine that remote connectivity users were authenticated via an authorized user account, password, and MFA token before establishing a VPN session.</p> <p>Inspected the IDS configurations and system dashboard to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|--|--|---|
| | | <p>The IDS is configured to notify appropriate IT personnel upon intrusion detection.</p> <p>A firewall is in place to filter unauthorized inbound network traffic from the internet.</p> <p>The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.</p> <p>Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.</p> <p>The centralized antivirus software is configured with continuous scanning and to automatically push updates when available.</p> | <p>Inspected the IDS alert notification configurations and an example IDS alert notification to determine that the IDS is configured to notify appropriate IT personnel upon intrusion detection.</p> <p>Inspected the network diagram and firewall rulesets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.</p> <p>Inspected the network diagram and firewall rulesets to determine the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.</p> <p>Inspected the antivirus software dashboard console and configurations to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.</p> <p>Inspected the antivirus software dashboard console and configurations to determine that the centralized antivirus software was configured with continuous scanning and to automatically push updates when available.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|---|--|---|
| | | <p>AWS load balancers are utilized to proxy traffic from the internet to internal IP addresses and for front load protection.</p> <p>Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.</p> <p>Transmission of data and digital output beyond the boundary of the system is secure through the use of encryption technologies and mechanisms.</p> <p>Critical data is stored in encrypted format using industry-standard AES-256 encryption algorithm.</p> <p>Stored passwords are encrypted with sha-256.</p> | <p>Inspected the encryption configurations and load balancers to determine that AWS load balancers were utilized to proxy traffic from the internet to internal IP addresses and for front load protection.</p> <p>Inspected the encryption configurations for data in transit and verified digital certification to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.</p> <p>Inspected the encryption policies and procedures, the encryption configurations, and the digital encryption certificates to determine that transmission of data and digital output beyond the boundary of the system was secure through the use of encryption technologies and mechanisms.</p> <p>Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using industry-standard AES-256 encryption algorithm.</p> <p>Inspected the password manager system and stored password encryption configurations to determine that stored passwords were encrypted with sha-256.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Logical and Physical Access Controls

| CC6.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|---|---|--|---|
| CC6.7 | The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. | <p>A DMZ is in place to isolate outside access and data from the entity's environment.</p> <p>Data backup and restore procedures are in place to guide personnel in performing backup activities and to guide personnel in system recovery activities.</p> <p>Backups of critical data are maintained securely offsite by the third-party cloud provider with multiple redundant locations.</p> <p>An automated backup system is in place to perform scheduled backups of data and systems.</p> <p>The ability to restore backed up data is restricted to authorized personnel.</p> | <p>Inspected the DMZ configurations to determine a DMZ was in place to isolate outside access and data from the entity's environment.</p> <p>Inspected the backup and restore policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities and to guide personnel in system recovery activities.</p> <p>Inspected the third-party attestation report to determine that backups of critical data were maintained offsite by the third-party cloud provider with multiple redundant locations.</p> <p>Inspected the backup schedule and configurations, the backup history, and an example backup log extract to determine that an automated backup system was in place to performed scheduled backups of data and systems.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding the list of users with the ability to restore backups to determine that the ability to restore backed up data was restricted to authorized personnel.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|--|---|---|
| | | <p>Backup data stores are configured to automatically expire on a set frequency.</p> <p>Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.</p> <p>Transmission of data and digital output beyond the boundary of the system is secure through the use of encryption technologies and mechanisms.</p> <p>Critical data is stored in encrypted format using industry-standard AES-256 encryption algorithm.</p> | <p>Inspected the list of users with the ability to restore backups to determine that the ability to restore backed up data was restricted to authorized personnel.</p> <p>Inspected the backup policy and procedures, the backup history and retention configurations, and an example backup log extract to determine that backup data stores were configured to automatically expire on a set frequency.</p> <p>Inspected the encryption configurations for data in transit and verified digital certification to determine that server certificate-based authentication was used as part of the TLS encryption with a trusted certificate authority.</p> <p>Inspected the encryption policies and procedures, the encryption configurations, and the digital encryption certificates to determine that transmission of data and digital output beyond the boundary of the system was secure through the use of encryption technologies and mechanisms.</p> <p>Inspected the encryption configurations for data at rest to determine that critical data was stored in encrypted format using industry-standard AES-256 encryption algorithm.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|--|---|---|
| | | <p>A firewall is in place to filter unauthorized inbound network traffic from the internet.</p> <p>The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.</p> <p>NAT functionality is utilized to manage internal IP addresses.</p> <p>An IDS is utilized to analyze network events and report possible or actual network security breaches.</p> <p>The IDS is configured to notify appropriate IT personnel upon intrusion detection.</p> <p>Policies and procedures are in place for remote access to systems from a mobile device.</p> | <p>Inspected the network diagram and firewall rulesets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.</p> <p>Inspected the network diagram and firewall rulesets to determine the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.</p> <p>Inspected the NAT configurations to determine that NAT functionality was utilized to manage internal IP addresses.</p> <p>Inspected the IDS configurations and system dashboard to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.</p> <p>Inspected the IDS alert notification configurations and an example IDS alert notification to determine that the IDS is configured to notify appropriate IT personnel upon intrusion detection.</p> <p>Inspected the remote access and mobile device security policies and procedures to determine that policies and procedures were in place for remote access to systems from a mobile device.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Logical and Physical Access Controls

| CC6.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|--|---|--|----------------------|
| CC6.8 | The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. | Mobile devices are protected through the use of secured, encrypted connections. | Inspected the remote access and mobile device security policies and procedures and the encryption policy and configurations for mobile devices to determine that mobile devices were protected through the use of secured, encrypted connections. | 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. |
| | | Access to implement changes into the production environment is restricted to authorized and appropriate personnel. | Inquired of the IT Infrastructure and Security Team Lead regarding access to implement changes in the production environment to determine that access to implement changes into the production environment was restricted to authorized and appropriate personnel. | No exceptions noted. |
| | | | Inspected the list of users with access to implement changes into the production environment to determine that access to implement changes into the production environment was restricted to authorized and appropriate 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 |
|-------|----------|--|---|---|
| | | <p>An IDS is utilized to analyze network events and report possible or actual network security breaches.</p> <p>The IDS is configured to notify appropriate IT personnel upon intrusion detection.</p> <p>Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.</p> <p>The centralized antivirus software is configured with continuous scanning and to automatically push updates when available.</p> | <p>Inspected the IDS configurations and system dashboard to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.</p> <p>Inspected the IDS alert notification configurations and an example IDS alert notification to determine that the IDS is configured to notify appropriate IT personnel upon intrusion detection.</p> <p>Inspected the antivirus software dashboard console and configurations to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.</p> <p>Inspected the antivirus software dashboard console and configurations to determine that the centralized antivirus software was configured with continuous scanning and to automatically push updates when available.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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. | <p>Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.</p> <p>Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.</p> <p>The monitoring software is configured to alert appropriate IT personnel when thresholds have been exceeded.</p> <p>An IDS is utilized to analyze network events and report possible or actual network security breaches.</p> | <p>Inspected the information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.</p> <p>Inspected the monitoring system and alert 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.</p> <p>Inspected the monitoring system notification configurations, dashboards, log reports, and an example monitoring alert notification to determine that the monitoring software was configured to alert appropriate IT personnel when thresholds had been exceeded.</p> <p>Inspected the IDS configurations and system dashboard to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|--|--|---|
| | | <p>The IDS is configured to notify appropriate IT personnel upon intrusion detection.</p> <p>A firewall is in place to filter unauthorized inbound network traffic from the internet.</p> <p>The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.</p> <p>Vulnerability scans are performed at least semi-annually on the environment to identify control gaps and vulnerabilities.</p> <p>A third party performs a penetration test annually to identify and exploit vulnerabilities identified within the environment.</p> | <p>Inspected the IDS alert notification configurations and an example IDS alert notification to determine that the IDS is configured to notify appropriate IT personnel upon intrusion detection.</p> <p>Inspected the network diagram and firewall rulesets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.</p> <p>Inspected the network diagram and firewall rulesets to determine the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.</p> <p>Inspected the completed vulnerability scan report and results to determine that vulnerability scans were performed at least semi-annually on the environment to identify control gaps and vulnerabilities.</p> <p>Inspected the completed third-party penetration test report and results to determine that a third party performed a penetration test annually to identify and exploit vulnerabilities identified within the environment.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

System Operations

| CC7.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|--------------|--|---|---|---|
| CC7.2 | <p>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.</p> | <p>Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.</p> <p>Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.</p> <p>The monitoring software is configured to alert appropriate IT personnel when thresholds have been exceeded.</p> <p>An IDS is utilized to analyze network events and report possible or actual network security breaches.</p> | <p>Inspected the information security and incident management policies and procedures to determine that policies and procedures were in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.</p> <p>Inspected the monitoring system and alert 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.</p> <p>Inspected the monitoring system notification configurations, dashboards, log reports, and an example monitoring alert notification to determine that the monitoring software was configured to alert appropriate IT personnel when thresholds had been exceeded.</p> <p>Inspected the IDS configurations and system dashboard to determine that an IDS was utilized to analyze network events and report possible or actual network security breaches.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|--|--|---|
| | | <p>The IDS is configured to notify appropriate IT personnel upon intrusion detection.</p> <p>A firewall is in place to filter unauthorized inbound network traffic from the internet.</p> <p>The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.</p> <p>Antivirus software is installed on workstations and servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.</p> <p>The centralized antivirus software is configured with continuous scanning and to automatically push updates when available.</p> | <p>Inspected the IDS alert notification configurations and an example IDS alert notification to determine that the IDS is configured to notify appropriate IT personnel upon intrusion detection.</p> <p>Inspected the network diagram and firewall rulesets to determine that a firewall was in place to filter unauthorized inbound network traffic from the internet.</p> <p>Inspected the network diagram and firewall rulesets to determine the firewall system was configured to deny any type of network connection that was not explicitly authorized by a firewall system rule.</p> <p>Inspected the antivirus software dashboard console and configurations to determine that antivirus software was installed on workstations and servers to detect and prevent the transmission of data or files that contained certain virus signatures recognized by the antivirus software.</p> <p>Inspected the antivirus software dashboard console and configurations to determine that the centralized antivirus software was configured with continuous scanning and to automatically push updates when available.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|---|--|--|--|
| | | Audit logging settings are in place for critical information system activity and events and logs are maintained and reviewed as needed. | Inquired of the IT Infrastructure and Security Team Lead regarding critical system audit logging to determine that audit logging settings were in place for critical information system activity and events, and that, logs were maintained and reviewed as needed. Inspected the system audit logging configurations and an example event audit log extract to determine that audit logging settings were in place for critical information system activity and events, and that, logs were maintained and reviewed as needed. | No exceptions noted. No exceptions noted. |
| | Corporate Network (Active Directory) | | | |
| | | Network account lockout settings are in place that include: <ul style="list-style-type: none"> • Account lockout duration • Account lockout threshold • Account lockout counter reset | Inspected the network account lockout settings to determine that network account lockout settings were in place that included: <ul style="list-style-type: none"> • 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 |
|-------|----------|--|---|---|
| | | <p>Network devices are configured to log events and access attempts to ensure that system activity can be traced to a specific user and that necessary data is available in the system logs to support audit and other related business functions.</p> <p>Network audit logging settings are in place for system events and sign-in activity and logs are maintained, monitored, and reviewed as needed.</p> | <p>Inspected the network audit and event logging configurations and an example audit log extract to determine that network devices were configured to log events and access attempts to ensure that system activity could be traced to a specific user and that necessary data was available in the system logs to support audit and other related business functions.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding corporate network audit and event logging to determine that network audit logging settings were in place for system events and sign-in activity and that logs were maintained, monitored, and reviewed as needed.</p> <p>Inspected the network audit and event logging configurations and an example audit log extract to determine that network audit logging settings were in place for system events and sign-in activity and that logs were maintained, monitored, and reviewed as needed.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|---|--|--|--|
| System Operations | | | | |
| CC7.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
| | Production Network (AWS) | | | |
| | | AWS audit logging settings are in place for usage and activity and logs are maintained and reviewed as needed. | Inquired of the IT Infrastructure and Security Team Lead regarding audit logging to determine that AWS audit logging settings were in place for usage and activity and that logs were maintained and reviewed as needed. Inspected the audit logging configurations and an example audit log extract to determine that AWS audit logging settings were in place for usage and activity and that logs were maintained and reviewed as needed. | No exceptions noted. No exceptions noted. |
| | Operating System (Amazon EC2 - CentOS Linux) | | | |
| | | Operating system account lockout settings are in place that include maximum authentication attempts and maximum sessions. Operating system audit logging settings are in place to record system authentication events and logs are maintained and reviewed as needed. | Inspected the operating system account lockout settings to determine that operating system account lockout settings were in place that included maximum authentication attempts and maximum sessions. Inquired of the IT Infrastructure and Security Team Lead regarding operating system audit logging to determine that operating system audit logging settings were in place to record system authentication events and logs were maintained and reviewed as needed. | No exceptions noted. 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 operating system audit logging configurations and an example audit log extract to determine that operating system audit logging settings were in place to record system authentication events and logs were maintained and reviewed as needed. | No exceptions noted. |
| Production Databases (Amazon RDS - PostgreSQL) | | | | |
| | | Database audit logging settings are in place for system activity and events, including logins, password failure, usage, and activity, and logs are maintained and reviewed as needed. | Inquired of the IT Infrastructure and Security Team Lead regarding database audit logs to determine that database audit logging settings were in place for system activity and events, including logins, password failure, usage, and activity, and that logs were maintained and reviewed as needed. Inspected the database audit logging configurations and an example audit log extract to determine that database audit logging settings were in place for system activity and events, including logins, password failure, usage, and activity, and that logs were maintained and reviewed as needed. | No exceptions noted. No exceptions noted. |

| TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY | | | | |
|---|--|--|--|---|
| System Operations | | | | |
| CC7.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
| | Application (Gtechna e-Citation Software) | | | |
| | | <p>Application account lockout settings are in place that include:</p> <ul style="list-style-type: none"> Invalid login threshold <p>Application audit logging settings are in place for system events and activity and logs are maintained and reviewed as needed.</p> | <p>Inspected the application account lockout configurations to determine that application account lockout settings were in place that included:</p> <ul style="list-style-type: none"> Invalid login threshold <p>Inquired of the IT Infrastructure and Security Team Lead regarding application audit logs to determine that application audit logging settings were in place for system events and activity and logs were maintained and reviewed as needed.</p> <p>Inspected the application audit logging configurations and an example audit log extract to determine application audit logging settings were in place for system events and activity and logs were maintained and reviewed as needed.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |
| | Remote Access and VPN (Cisco AnyConnect) | | | |
| | | <p>VPN audit logging is enabled to provide event history for VPN activity and logs are maintained and reviewed as needed.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding VPN audit logging to determine that VPN audit logging was enabled to provide event history for VPN activity and logs were maintained and reviewed as needed.</p> | <p>No exceptions noted.</p> |

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. | <p>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.</p> <p>Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place, made available, and communicated to appropriate users.</p> | <p>Inspected the VPN logging configurations and an example event log extract to determine that VPN audit logging was enabled to provide event history for VPN activity and logs were maintained and reviewed as needed.</p> <p>Inspected the incident response and escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.</p> <p>Inspected the incident response and escalation policies and procedures, the entity's intranet, the entity's support portal, and the customer terms and agreement template to determine that documented escalation procedures for reporting system failures, incidents, concerns, and other complaints were in place, made available, and communicated to appropriate users.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|---|---|---|
| | | <p>Documented incident response policies and procedures are in place to guide personnel in the event of an incident.</p> <p>The incident response and escalation procedures define the classification of incidents based on its severity.</p> <p>Incidents are documented and tracked in a ticketing system and updated to reflect the planned incident and problem resolution.</p> <p>Significant events and incidents are reviewed, monitored, and investigated by an incident response team.</p> | <p>Inspected the incident response policies and procedures to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident.</p> <p>Inspected the incident response and escalation policies and procedures to determine that the incident response and escalation procedures defined the classification of incidents based on its severity.</p> <p>Inspected the incident response and escalation policies and procedures and the incident tracking tool to determine that incidents were documented and tracked in a ticketing system and updated to reflect the planned incident and problem resolution.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding incident response and management procedures to determine that significant events and incidents were reviewed, monitored, and investigated by an incident response team.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|---|--|--|
| | | <p>Identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p> | <p>Inspected the incident response and management policies and procedures to determine that significant events and incidents were reviewed, monitored, and investigated by an incident response team.</p> <p>Inspected the supporting ticket for a sample of significant events to determine that significant events and incidents were reviewed, monitored, and investigated by an incident response team.</p> <p>Inspected the supporting incident ticket for a sample of security incidents to determine that significant events and incidents were reviewed, monitored, and investigated by an incident response team.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding incident response and management procedures to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p> | <p>No exceptions noted.</p> <p>Testing of the control activity disclosed that no significant security events had occurred during the review period.</p> <p>Testing of the control activity disclosed that no security incidents had occurred during the review period.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|---|--|--|
| | | <p>Resolution of significant events and incidents is documented within the ticket and communicated to affected users.</p> | <p>Inspected the incident response policies and procedures to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p> <p>Inspected the supporting incident ticket and log for a sample of security incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding incident response and management procedures to determine that the resolution of significant events and incidents was documented within the ticket and communicated to affected users.</p> | <p>No exceptions noted.</p> <p>Testing of the control activity disclosed that no security incidents had occurred during the review period.</p> <p>No exceptions noted.</p> |

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 |
|--------------|-----------------|--|---|---|
| | | <p>A security incident analysis is performed for critical incidents to determine the root cause, system impact, and to determine the resolution.</p> | <p>Inspected the incident response and management policies and procedures to determine that the resolution of significant events and incidents was documented within the ticket and communicated to affected users.</p> <p>Inspected the supporting ticket for a sample of significant events to determine that the resolution of significant events and incidents was documented within the ticket and communicated to affected users.</p> <p>Inspected the supporting incident ticket for a sample of security incidents to determine that the resolution of significant events and incidents was documented within the ticket and communicated to affected users.</p> <p>Inquired of the IT Infrastructure and Security Team Lead regarding incident response and management procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact, and to determine the resolution.</p> | <p>No exceptions noted.</p> <p>Testing of the control activity disclosed that no significant security events had occurred during the review period.</p> <p>Testing of the control activity disclosed that no critical security incidents had occurred during the review period.</p> <p>No exceptions noted.</p> |

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. | <p>Inspected the incident response and management policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact, and to determine the resolution.</p> <p>Inspected the supporting incident ticket for a sample of security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact, and to determine the resolution.</p> <p>Inspected the incident response and escalation policies and procedures to determine that documented incident response and escalation procedures for reporting security incidents were in place to guide users in identifying, reporting, and mitigating failures, incidents, concerns, and other complaints.</p> | <p>No exceptions noted.</p> <p>Testing of the control activity disclosed that no critical security incidents had occurred during the review period.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

System Operations

| CC7.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|----------|--|---|----------------------|
| | | Documented escalation procedures for reporting system failures, incidents, concerns, and other complaints are in place, made available, and communicated to appropriate users. | Inspected the incident response and escalation policies and procedures, the entity's intranet, the entity's support portal, and the customer terms and agreement template to determine that documented escalation procedures for reporting system failures, incidents, concerns, and other complaints were in place, made available, and communicated to appropriate users. | No exceptions noted. |
| | | Documented incident response policies and procedures are in place to guide personnel in the event of an incident. | Inspected the incident response policies and procedures to determine that documented incident response policies and procedures were in place to guide personnel in the event of an incident. | No exceptions noted. |
| | | The incident response and escalation procedures define the classification of incidents based on its severity. | Inspected the incident response and escalation policies and procedures to determine that the incident response and escalation procedures defined the classification of incidents based on its severity. | No exceptions noted. |
| | | Incidents are documented and tracked in a ticketing system and updated to reflect the planned incident and problem resolution. | Inspected the incident response and escalation policies and procedures and the incident tracking tool to determine that incidents were documented and tracked in a ticketing system and updated to reflect the planned incident and problem resolution. | No exceptions noted. |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

System Operations

| CC7.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|----------|---|--|--|
| | | <p>Significant events and incidents are reviewed, monitored, and investigated by an incident response team.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding incident response and management procedures to determine that significant events and incidents were reviewed, monitored, and investigated by an incident response team.</p> <p>Inspected the incident response and management policies and procedures to determine that significant events and incidents were reviewed, monitored, and investigated by an incident response team.</p> <p>Inspected the supporting ticket for a sample of significant events to determine that significant events and incidents were reviewed, monitored, and investigated by an incident response team.</p> <p>Inspected the supporting incident ticket for a sample of security incidents to determine that significant events and incidents were reviewed, monitored, and investigated by an incident response team.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>Testing of the control activity disclosed that no significant security events had occurred during the review period.</p> <p>Testing of the control activity disclosed that no security incidents had occurred during the review period.</p> |

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 |
|-------|----------|---|--|--|
| | | <p>Identified incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding incident response and management procedures to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p> <p>Inspected the incident response policies and procedures to determine that identified incidents were analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p> <p>Inspected the supporting incident ticket and log for a sample of security incidents to determine that identified incidents were analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>Testing of the control activity disclosed that no security incidents had occurred during the review period.</p> |

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 |
|-------|----------|---|--|---|
| | | <p>Resolution of significant events and incidents is documented within the ticket and communicated to affected users.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding incident response and management procedures to determine that the resolution of significant events and incidents was documented within the ticket and communicated to affected users.</p> <p>Inspected the incident response and management policies and procedures to determine that the resolution of significant events and incidents was documented within the ticket and communicated to affected users.</p> <p>Inspected the supporting ticket for a sample of significant events to determine that the resolution of significant events and incidents was documented within the ticket and communicated to affected users.</p> <p>Inspected the supporting incident ticket for a sample of security incidents to determine that the resolution of significant events and incidents was documented within the ticket and communicated to affected users.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>Testing of the control activity disclosed that no significant security events had occurred during the review period.</p> <p>Testing of the control activity disclosed that no critical security incidents had occurred during the review period.</p> |

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 |
|-------|---|---|---|---|
| CC7.5 | The entity identifies, develops, and implements activities to recover from identified security incidents. | <p>A security incident analysis is performed for critical incidents to determine the root cause, system impact, and to determine the resolution.</p> <p>Documented change control policies and procedures are in place to guide personnel in the change management process.</p> | <p>Inquired of the IT Infrastructure and Security Team Lead regarding incident response and management procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact, and to determine the resolution.</p> <p>Inspected the incident response and management policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact, and to determine the resolution.</p> <p>Inspected the supporting incident ticket for a sample of security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact, and to determine the resolution.</p> <p>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.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>Testing of the control activity disclosed that no critical security incidents had occurred during the review period.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

System Operations

| CC7.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|----------|--|---|----------------------|
| | | Change management requests are opened for incidents that require permanent fixes. | Inspected the change management and incident response and management policies and procedures to determine that change management requests were required to be opened for incidents that required permanent fixes. | No exceptions noted. |
| | | Data backup and restore procedures are in place to guide personnel in performing backup activities and to guide personnel in system recovery activities. | Inspected the backup and restore policies and procedures to determine that data backup and restore procedures were in place to guide personnel in performing backup activities and to guide personnel in system recovery activities. | No exceptions noted. |
| | | A security incident analysis is performed for critical incidents to determine the root cause, system impact, and to determine the resolution. | Inquired of the IT Infrastructure and Security Team Lead regarding incident response and management procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact, and to determine the resolution. | No exceptions noted. |
| | | | Inspected the incident response and management policies and procedures to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact, and to determine the resolution. | No exceptions noted. |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

System Operations

| CC7.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|----------|---|---|---|
| | | <p>Business continuity and disaster recovery plans are developed and updated on an annual basis.</p> <p>Data backup restoration tests are performed on an annual basis.</p> | <p>Inspected the supporting incident ticket for a sample of security incidents to determine that a security incident analysis was performed for critical incidents to determine the root cause, system impact, and to determine the resolution.</p> <p>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.</p> <p>Inspected the completed backup restoration test to determine that data backup restoration tests were performed on an annual basis.</p> | <p>Testing of the control activity disclosed that no critical security incidents had occurred during the review period.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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. | <p>Documented change control policies and procedures are in place to guide personnel in the change management process.</p> <p>The change management process has defined roles for approval, development, testing, and deployment.</p> <p>System change requests are documented and tracked in a ticketing system.</p> <p>System changes are authorized and approved by management prior to implementation.</p> | <p>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.</p> <p>Inspected the change management policies and procedures to determine that the change management process had defined roles for approval, development, testing and deployment.</p> <p>Inspected the change management policies and procedures and the supporting change ticket for a sample of system changes to determine that system change requests were documented and tracked in a ticketing system.</p> <p>Inspected the change management policies and procedures and the supporting change ticket for a sample of system changes to determine that system changes were authorized and approved by management prior to implementation.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Change Management

| CC8.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|----------|--|--|----------------------|
| | | System changes are tested prior to implementation. Types of testing performed depend on the nature of the change. | Inspected the change management policies and procedures and 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. |
| | | Development and test environments are physically and logically separated from the production environment. | Inspected the separate development, Quality Assurance (QA) and production environments to determine that development and test environments were physically and logically separated from the production environment. | No exceptions noted. |
| | | Access to implement changes into the production environment is restricted to authorized and appropriate personnel. | Inquired of the IT Infrastructure and Security Team Lead regarding access to implement changes in the production environment to determine that access to implement changes into the production environment was restricted to authorized and appropriate personnel. | No exceptions noted. |
| | | | Inspected the list of users with access to implement changes into the production environment to determine that access to implement changes into the production environment was restricted to authorized and appropriate personnel. | No exceptions noted. |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Change Management

| CC8.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|----------|--|--|---|
| | | <p>Changes implemented into the production environment trigger an automated alert to appropriate users.</p> <p>Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.</p> <p>Rollback capability and back out procedures are in place in the event that system changes impair system operations or do not function as designed.</p> <p>Access to source code is restricted to authorized personnel.</p> | <p>Inspected the change control alerting configurations and an example alert to determine that changes implemented into the production environment triggered an automated alert to appropriate users.</p> <p>Inspected the change control code 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.</p> <p>Inspected the rollback and back out procedures to determine that rollback capability and back out procedures were in place in the event that system changes impaired system operations or did not function as designed.</p> <p>Inquired of the IT Infrastructure and Security Lead regarding authorized personnel with access to source code to determine that access to source code was restricted to authorized personnel.</p> <p>Inspected the listing of users with access to source code to determine that access to source code was restricted to authorized personnel.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|--|---|---|
| | | <p>System changes are communicated to both affected internal and external users.</p> <p>Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.</p> | <p>Inspected the internal change communication via change tickets, slack, and e-mail and the external change communication via the support portal and release notes to determine that system changes were communicated to both affected internal and external users.</p> <p>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.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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. | <p>Documented policies and procedures are in place to guide personnel in performing risk mitigation activities.</p> <p>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.</p> <p>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.</p> <p>Identified risks are rated using a risk analysis and evaluation process.</p> | <p>Inspected the risk assessment and management policies and procedures to determine that documented policies and procedures were in place to guide personnel in performing risk mitigation activities.</p> <p>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.</p> <p>Inspected the risk assessment policies and procedures and 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.</p> <p>Inspected the risk assessment policies and procedures and the completed risk assessment to determine that identified risks were rated using a risk analysis and evaluation process.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Risk Mitigation

| CC9.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|--|---|--|----------------------|
| CC9.2 | The entity assesses and manages risks associated with vendors and business partners. | Risks identified as a part of the risk assessment process are addressed using one of the following strategies: <ul style="list-style-type: none"> • Avoid the risk • Accept the risk • Reduce the risk | Inspected the risk assessment policies and procedures and the completed risk assessment to determine that risks identified as a part of the risk assessment process were addressed using one of the following strategies: <ul style="list-style-type: none"> • Avoid the risk • Accept the risk • Reduce the risk | No exceptions noted. |
| | | Management develops risk mitigation strategies to address risks identified during the risk assessment process. | Inspected the risk assessment, management, and mitigation 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. |
| | | 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 certificate of liability insurance to determine that the entity purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability. | No exceptions noted. |
| | | Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances. | Inspected the vendor risk assessment and management policies and procedures to determine that management defined a third-party vendor risk management process that specified the process for evaluating third-party risks based on identified threats and the specified tolerances. | No exceptions noted. |

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

Risk Mitigation

| CC9.0 | Criteria | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|-------|----------|--|---|---|
| | | <p>Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>Identified third-party risks are rated using a risk evaluation process and ratings are approved by management as needed.</p> <p>Agreements are in place with third parties to:</p> <ul style="list-style-type: none"> • Delineate the boundaries of the system and describe relevant system components • Communicate the system commitments and requirements • Outline and communicate the terms, conditions, and responsibilities | <p>Inspected the vendor risk assessment and management policies and procedures and the completed third-party risk assessment to determine that management developed third-party risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>Inspected the vendor risk assessment and management policies and procedures and the completed third-party risk assessment to determine that identified third-party risks were rated using a risk evaluation process and ratings were approved by management as needed.</p> <p>Inspected the third-party agreement templates and the executed agreement for a sample of third parties to determine that agreements were in place with third parties to:</p> <ul style="list-style-type: none"> • Delineate the boundaries of the system and describe relevant system components • Communicate the system commitments and requirements • Outline and communicate the terms, conditions, and responsibilities | <p>No exceptions noted.</p> <p>No exceptions noted.</p> <p>No exceptions noted.</p> |

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 |
|-------|----------|--|---|---|
| | | <p>Vendor systems are subject to review as part of the vendor risk management process. Attestation reports are obtained and evaluated when available for high-risk or critical vendors.</p> <p>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.</p> | <p>Inspected the vendor risk assessment and management policies and procedures and the completed third-party risk assessment including critical vendor attestation report review to determine that vendor systems were subject to review as part of the vendor risk management process, and that, attestation reports were obtained and evaluated when available for high-risk or critical vendors.</p> <p>Inspected the risk assessment policies and procedures and 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.</p> | <p>No exceptions noted.</p> <p>No exceptions noted.</p> |